TS 101 009 V1.1.1 (1997-11)

Technical specification

Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Types and characteristics

European Telecommunications Standards Institute

Reference

DTS/TM-03025 (9cc00icr.PDF)

Keywords

SDH, transmission, network, protection, protocol,
interworking

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

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 the Transmission and Multiplexing (TM) Technical Committee of the European Telecommunications Standards Institute (ETSI).

The present document has been produced to give guidance to network operators and equipment manufacturers on Synchronous Digital Hierarchy (SDH) network protection schemes. It is one of a family of related TSs and 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 [1]: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Interworking - rings and other schemes".

ETS 300 746 [2]: "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 functional requirements and classification of Synchronous Digital Hierarchy (SDH) protection schemes, namely SDH multiplex section trail shared protection ring, multiplex section trail dedicated protection ring, multiplex section trail linear protection, and Lower Order/Higher Order (LO/HO) Virtual Container (VC) trail and Sub-Network Connection (SNC) protection schemes. The various SDH protection schemes are specified in terms of their network objectives, network architectures, functional modelling and network operations.

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 101 010 (1997): "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Interworking - rings and other schemes".

[2] ETS 300 746 (1997): "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.708: "Network node interface for the synchronous digital hierarchy".

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1 General definitions

Administrative Unit (AU): See ITU-T Recommendation G.708 [4].

Administrative Unit Group (AUG): See ITU-T Recommendation G.708 [4].

Automatic Protection Switching (APS): See ITU-T Recommendation G.783 [6].

bi-directional connection: As defined in ITU-T Recommendation G.803 [3] (A connection consisting of an associated pair of unidirectional connections capable of simultaneously transferring information in opposite directions betwen their respective inputs and outputs). This connection can be uniformly or diversely routed.

Bit Interleaved Parity (BIP): See ITU-T Recommendation G.708 [4].

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

bridge request: A request sent by the tail-end node to the head-end node to perform a bridge.

consolidation: The allocation of server layer trails to client layer connections which ensures that each server layer trail is full before the next is allocated. Consolidation minimises the number of partially filled server layer trails. It therefore maximises the "fill factor". Thus a number of partially filled Virtual Container, level 4 (VC-4) paths may be consolidated into a single, fully filled VC-4.

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

diverse routeing: Bidirectional working traffic (ie. go and return) is transported on different physical facilities under non-failure conditions. Such routeing may apply to individual trails or SNCs (see figure 2).

dual ended operation: See ITU-T Recommendation G.803 [3].

grooming: The allocation of server layer trails to client layer connections which groups together client layer connections whose characteristics are similar or related. (Thus it is possible to groom VC-12 paths by service type, by destination, or by protection category in to particular VC-4 paths which can then be managed accordingly. It is also possible to groom VC-4 paths according to similar criteria into Synchronous Transport Module (level) N (STM-N) sections).

head-end: The node that executes a bridge.

Loss Of Frame (LOF): See ITU-T Recommendation G.783 [6].

Loss Of Signal (LOS): See ITU-T Recommendation G.783 [6].

lower order Virtual Container (VC) access: The termination of a higher order VC for the purpose of adding, dropping, or cross-connecting any individual Lower Order (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 [3].

Multiplex Section - Alarm Indication Signal (MS-AIS): See ITU-T Recommendation G.783 [6].

Multiplex Section - Far End Receive Failure (MS-FERF): See ITU-T Recommendation G.709 [5].

Network Node Interface (NNI): See ITU-T Recommendation G.708 [4].

non-revertive operation: In the non-revertive mode of operation, the working traffic remains on the protection trail/SNC when the working trail/SNC has recovered from a fault.

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 [3].

path AIS: See ITU-T Recommendation G.783 [6].

Path OverHead (POH): See ITU-T Recommendation G.708 [4].

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

protection trail: The trail allocated to transport the 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].

revertive operation: In the revertive mode of operation, the traffic on the protection trail/sub-network connection shall be switched back to the working trail/sub-network connection when this working trail/sub-network connection has recovered from a fault.

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 secondary 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 [4].

Section Termination (ST): See ITU-T Recommendation G.803 [3].

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

single ended operation: See ITU-T Recommendation G.803 [3].

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 [3].

Sub-Network Connection (SNC) protection: See ITU-T Recommendation G.803 [3].

switch: The action of selecting traffic from the protection trail/sub-network connection rather than the working trail/sub-network connection.

switch completion time: See ITU-T Recommendation G.841 [7].

switching node: See ITU-T Recommendation G.841 [7].

tail-end: The node that requests the bridge.

timeslot interchange: Timeslot interchange is 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 [3].

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

Tributary Unit (TU): See ITU-T Recommendation G.708 [4].

Tributary Unit Group (TUG): See ITU-T Recommendation G.708 [4].

unidirectional connection: As defined in ITU-T Recommendation G.803 [3] (A connection which is capable of transparently transferring information from input to output) (see figure 1).

uniform routeing: Bidirectional working traffic (i.e. go and return) is transported on the same physical facilities under non-failure conditions (see figure 2).

Virtual Container (VC): See ITU-T Recommendation G.708 [4].

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

working Sub-Network Connection (SNC): The sub-network connection over which traffic is transported when there is no switch event.

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 traffic is transported when there is no switch event.

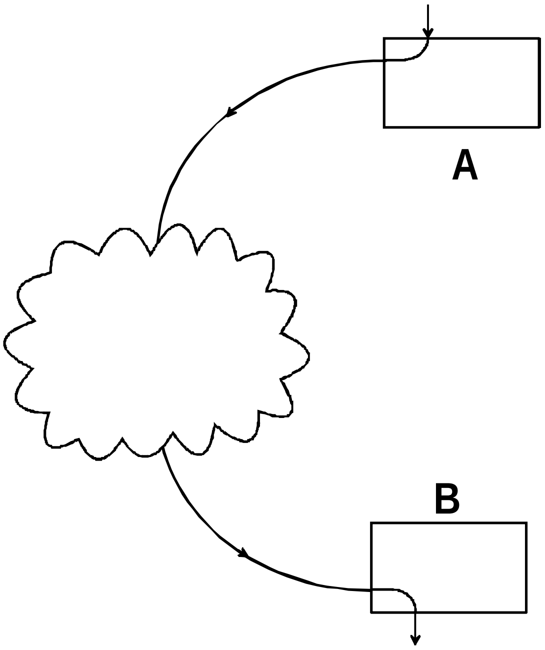
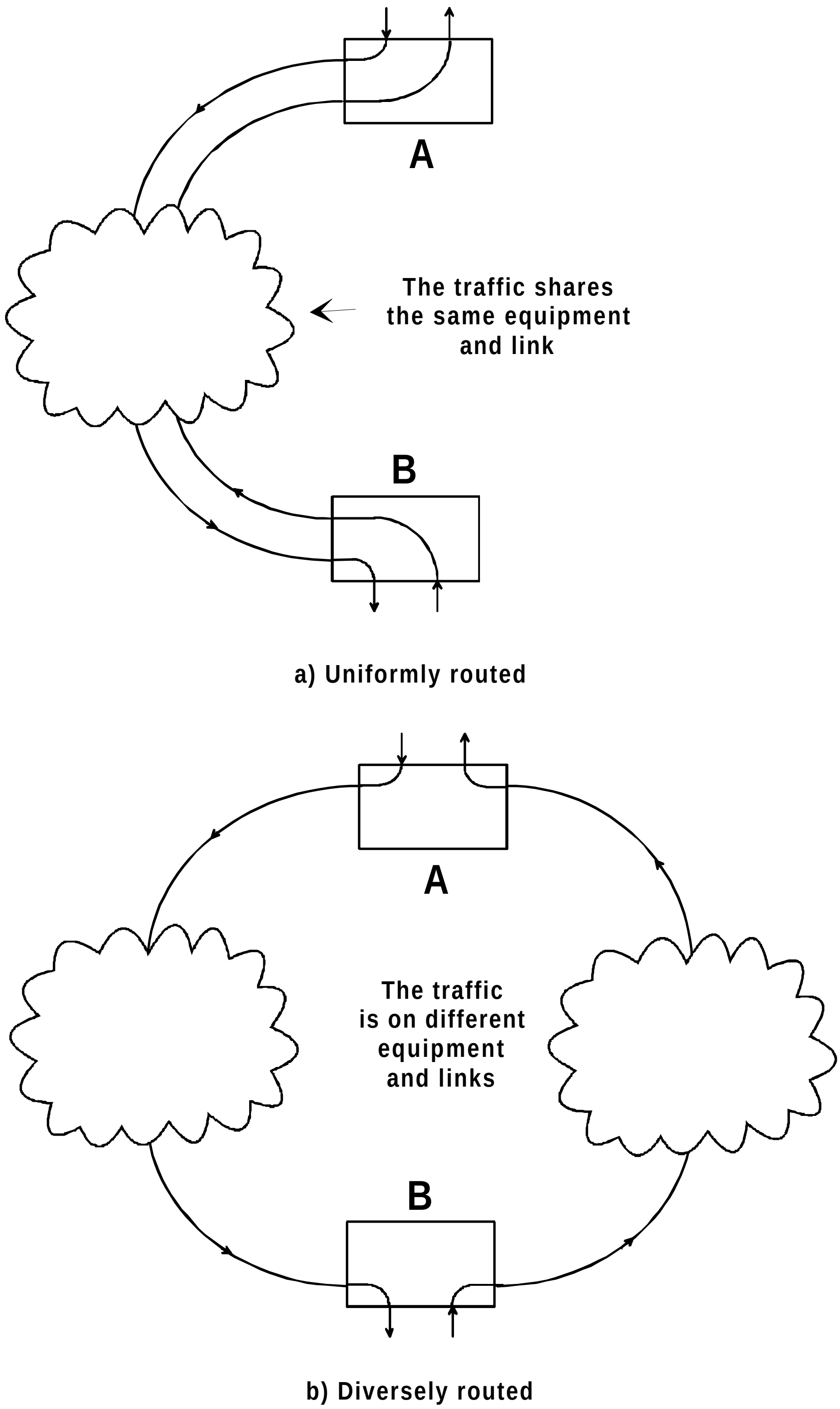


Figure 1: Unidirectional connection



a) Uniformly routed

b) Diversely routed

Figure 2: Uniformly routed and diversely routed bi-directional connection

3.1.2 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 between any pair of nodes of the ring 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 on the long path 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.

3.2 Abbreviations

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

ADM	Add Drop Multiplexer
AIS	Alarm Indication Signal
AP	Access Point
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
BSHR	Bidirectional Self Healing Ring
CP	Connection Point
CPE	Customer Premises Equipment
DXC	Digital Cross-Connect
EXER	Exercise
EXER-R	Exercise - Ring
FEBE	Far End Block Error
FERF	Far End Receive Failure
FS	Forced Switch (of working to protection)
FS-R	Forced Switch (of working to protection) - Ring
HO	Higher Order
HPA	Higher order Path Adaptation
HPT	Higher order Path Termination
HPC	Higher order Path Connection
LP	Lock out of Protection
LPA	Lower order Path Adaptation
LPC	Lower order Path Connection
LPT	Lower order Path Termination
LO	Lower Order
LOF	Loss Of Frame
LOS	Loss Of Signal
MCp	Matrix Connection
MS	Multiplex Section
MSA	Multiplex Section Adaptation
MS-BSHR	Multiplex Section - Bidirectional Self Healing Ring
MS DPRing	Multiplex Section trail Dedicated Protection Ring
MS SPRing	Multiplex Section Shared Protection Ring
MSPA	Multiplex Section Protection Adaptation
MSPT	Multiplex Section Protection Termination

MS-R	Manual Switch (of working to protection) - Ring
MST	Multiplex Section Termination
MS-USHR	Multiplex Section - Unidirectional Self Healing Ring
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
PSTN	Public Switched Telephone Network
RC	Remote Concentrator
RR	Reverse Request
RR-R	Reverse Request - Ring
RS	Regenerator Section
SD	Signal Degrade
SD-R	Siefgnal Degrade - Ring
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SF-R	Signal Fail - Ring
SNC	Sub-Network Connection
SNC/I	Inherently monitored Sub-Network Connection protection
SNC/N	Non-intrusively monitored Sub-Network Connection protection
SOH	Section OverHead
SA	Section Adaptation
SPRing	Shared Protection Ring
ST	Section Termination
STM	Synchronous Transport Module
STM-N	Synchronous Transport Module (level) N
TCP	Termination Connection Point
TSI	Timeslot Interchange
TT	Termination supervision
TU	Tributary Unit
TU-AIS	Tributary Unit - Alarm Indication Signal
TUG	Tributary Unit Group
TU-n	Tributary Unit (level) n
USHR	Unidirectional Self Healing Ring
VC-n	Virtual Container (level) n
WTR	Wait To Restore

4 Protection classifications and traffic patterns

4.1 Protection classifications

SDH protection schemes can be classified, using the layering concept of a transport network model in ITU-T Recommendation G.803 [3], into the MS protection and the path protection schemes.

4.1.1 Multiplex Section (MS) trail protection

MS trail protection provides end-to-end protection of MS trail by means of an MS trail protection sub-layer. The trail termination function at the MS layer is expanded to form the trail protection sub-layer.

The network applications of MS trail protection are either linear point-to-point protection or ring protection.

4.1.1.1 MS trail linear protection

Linear point-to-point protection in the MS layer network, in functional modelling, are termed MS trail linear protection.

4.1.1.2 MS trail protection ring

SDH rings in the MS layer network, in functional modelling, are termed MS trail protection rings.

There are two MS trail protection ring architectures: MS trail shared protection ring and MS trail dedicated protection ring. They are characterised by the directionality of the traffic carried around the ring and the protection scheme used to effect the protection switch.

4.1.1.2.1 MS trail shared protection ring

MS trail shared protection ring is a shared MS protection ring (1:n) in which the total capacity in a multiplex section is divided equally into working and protection capacity. The protection capacity in a multiplex section is shared to protect the working traffic carried in the working capacity of any multiplex section in the ring. The MS trail shared protection ring is sometimes referred to as a MS Shared Protection Ring (MS SPRing) or a MS Bidirectional Self Healing Ring (MS-BSHR).

4.1.1.2.2 MS trail dedicated protection ring

MS trail dedicated protection ring is a dedicated MS protection ring because it provides one dedicated protection entity for each working entity (1+1 or 1:1). The MS trail dedicated protection ring is sometimes referred to as MS Dedicated Protection Ring (MS DPRing) or a MS Unidirectional Self Healing Ring (MS-USHR).

4.1.2 Path protection

There are two path layer networks: the LO path layer network and the Higher Order (HO) path layer network. The protection schemes in the path layers are termed LO path protection and HO path protection. The LO/HO protection schemes can be further classified, using the partitioning concept of a transport network model in ITU-T Recommendation G.803 [3], into the LO/HO trail protection and the LO/HO SNC protection.

4.1.2.1 LO/HO trail protection

This is end-to-end protection of a LO or HO VC, by means of a LO or HO trail protection sub-layer. The trail termination function at the LO/HO path layer is expanded to form the trail protection sub-layer.

4.1.2.2 LO/HO Sub-Network Connection (SNC) protection

In this case the connection point at the LO/HO layer is expanded to provide a monitoring function for SNC.

4.1.2.3 Single ended and dual ended switching

Possible advantages of single ended switching when both directions of transmission use the same equipment (i.e. the working and protection trails are bi-directional) include:

1) single ended switching is a simple scheme to implement and does not require a protocol;

2) single ended switching can be faster than dual ended switching because it does not require a protocol;

3) different equipment is used for each direction of transmission after a failure and therefore the number of breaks, resulting from multiple failures, will be less than if both directions of transmission use the same equipment.

Possible advantages of dual-ended switching when both directions of transmission use the same equipment (i.e. the working and protection trails are bi-directional) include:

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

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

c) dual ended switching is easier to manage because both directions of transmission use the same equipments along the full length of the trail;

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

Dual-ended protection should not be used with VC trail protection trail rings because none of the above advantages would be realized.

Both single ended and dual ended switching operation and interworking with other protection mechanisms are for further study.

4.1.3 Revertive/non-revertive operation

Some protection schemes are inherently revertive. For other schemes either revertive or non-revertive operation is possible. An advantage of non-revertive operation is that, in general, it will introduce fewer breaks. However, there are situations where revertive operation may be preferred. Examples of cases where revertive operation may be appropriate are:

1) where parts of the protection channel (i.e. a SNC, or VC/MS trail) may be taken to provide capacity to meet a more urgent need. For example, where protection channels can be taken out of service to release capacity for use in restoring other traffic;

2) where the protection channel may be subject to frequent re-arrangement. For example, where a network has limited capacity and protection routes are frequently re-arranged to maximize network efficiency when changes occur in the network;

3) where the protection channel is of significantly lower performance than the main channel. For example, where the protection channel has a worse error performance or longer delay than the normal working channel;

4) when an operator needs to know which channels are carrying traffic in order to simplify the management of the network.

4.1.4 Optical protection switching

Optical protection switching is an optical layer protection scheme. It is not restricted to use only with SDH.

This scheme is for further study.

4.2 Traffic patterns for rings

Four traffic patterns that are typical of transport network applications are illustrated in figure 3.

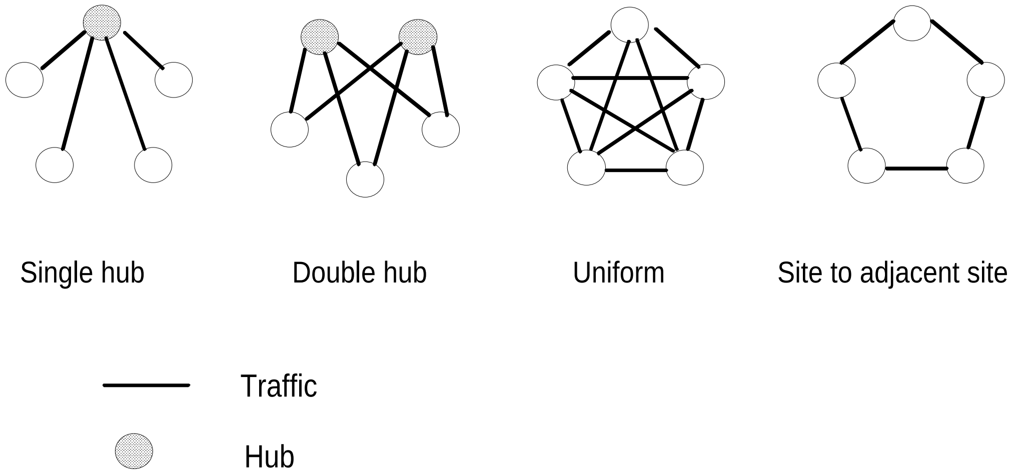


Figure 3: Traffic patterns

4.2.1 Single hub

All traffic goes to a single site, called a hub. This is typical for sub-networks in the periphery of some metropolitan networks and in local/access networks.

4.2.2 Double hub

All traffic goes to two nodes, called hubs. An example of an application is when a local exchange is connected to two higher level exchanges in order to protect the user traffic against the failure of one of the higher level exchanges. For the purpose of this report it is assumed that there is no traffic between the hubs.

4.2.3 Uniform

Traffic is evenly distributed between sites. Every site has approximately the same level of traffic to every other site. This is typical for sub-networks in metropolitan and core or backbone network applications where the sites share a common community of interest.

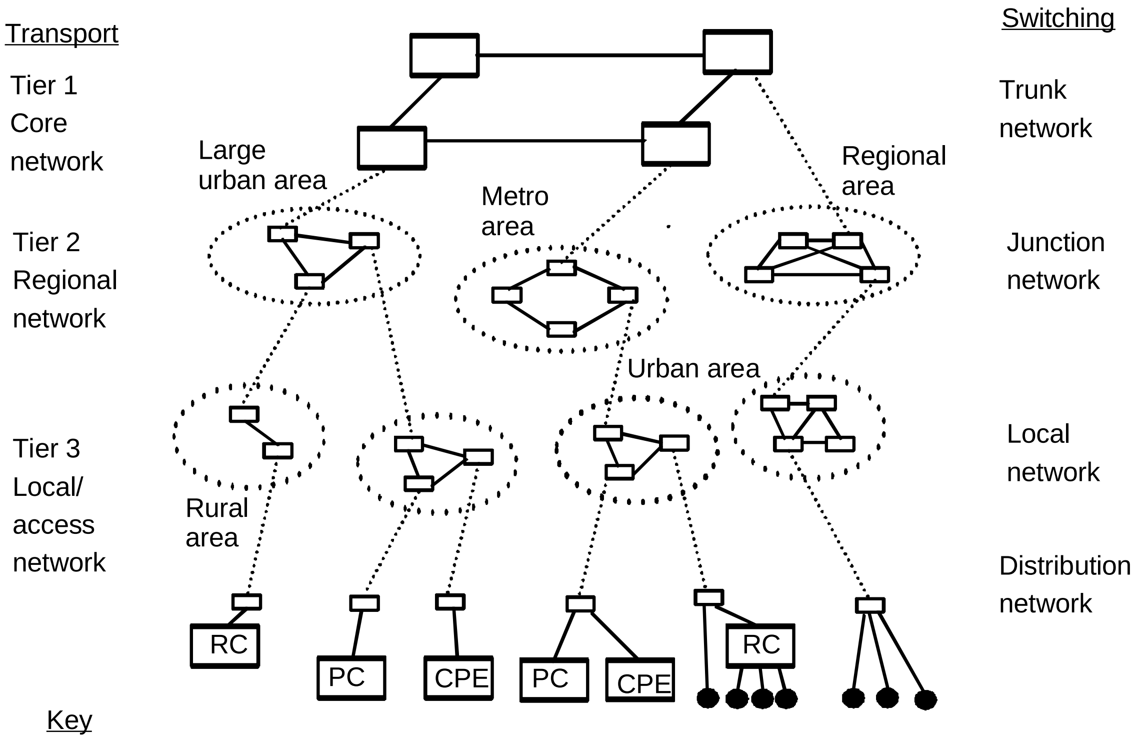
4.2.4 Site to adjacent site

Traffic goes from every site to its neighbour sites. This is a common traffic pattern where the traffic demand between adjacent sites is high, for example between major cities in a core or backbone network, or where only major offices within a city are connected to the sub-network.

5 Network requirements for protection

An SDH transport network structure is required to identify the applications of SDH sub-networks. A model of the network structure is shown in figure 4. It is an abstract network structure in that it does not imply the physical realization of each level or tier of the network model, since these can have individual transport infrastructures.

The structure of the SDH transport network can be characterized as comprising three network tiers, namely the tier 1 core network, tier 2 regional network and the tier 3 local/access network. They correspond approximately to the trunk, junction and local/distribution networks in a switching hierarchy.



Key

RC - Remote Concentrator
PC - Private Circuits
CPE - Customer Premises Equipment
● - Subscribers

Figure 4: A model of an SDH transport network structure

5.1 Core network

This is the tier 1 core or backbone network used for transporting high capacity inter-regional traffic and international traffic.

The tier 1 network can consist of a mesh of Digital Cross Connects (DXCs) interconnected by line systems and/or ring networks.

5.2 Regional network

This is the tier 2 regional network used for transporting traffic in different geographical regions such as large urban or metropolitan areas of a country.

In this region, rings or mesh networks with DXCs can be used to provide traffic routeing flexibility in addition to network protection, by grooming and consolidating LO VC traffic.

5.3 Local/access network

This is the tier 3 local/access network used for transporting low capacity local traffic in smaller urban and rural areas, and collecting traffic from the access network.

In this network, rings can also provide traffic routeing flexibility in addition to network protection, by grooming and consolidating 2 Mbit/s PC and Public Switched Telephone Network (PSTN) traffic. PSTN traffic is routed to a local exchange. PC traffic is consolidated into Synchronous Transport Module (level)-1 (STM-1) circuits and then either routed to another tier 3 local/access network ring or routed to the tier 2 regional network for onward distribution.

5.4 General protection objectives

The general objectives for protection include:

1 to improve service availability:

1.1 protection of traffic over critical links and sub-networks;

- protection of high capacity links in the core network;
- protection of traffic over sub-networks or operator domains;
- protection of traffic between sub-networks;
- protection of traffic from customer sites where high reliability is required;
- end to end protection of selected links which require high reliability (e.g. private circuits).

1.2 to protect selected VCs within a HO VC.

2 to facilitate maintenance;

3 to facilitate in-service network upgrade.

NOTE: The most probable fault causes in the core network are cable cuts, due to digging up or other human activity, and optical component failures which account for a large percentage of the total faults in the network, as shown also in some recent ITU-T contributions (SG15 meeting, May 1994).

6 Multiplex section trail protection schemes

6.1 Multiplex section trail linear protection

Two MS trail linear protection schemes are described in ITU-T Recommendation G.803 [3]. These are linear MS trail 1+1 and 1:N protection schemes.

The APS protocols of these schemes are described in ETS 300 746 [2].

6.2 Two-fibre MS SPRing

6.2.1 Network architecture

A MS SPRing uses uniform routeing so that the working traffic is transported over the bi-directional MS working trails. In the event of a failure, interrupted traffic is transported over the bi-directional MS protection trails in the opposite direction around the ring.

It is a shared MS protection ring (1:n) in which the total capacity of N Administrative Unit Groups (AUGs) in a multiplex section is divided equally into N/2 working and N/2 protection AUGs. Under a protection switch, the AUG working channels numbered 1 to N/2 are switched into the protection channels N/2 + 1 to N. The protection capacity in a multiplex section is shared to protect the working traffic carried in the working capacity of any multiplex section in the ring.

In case of a uniform or site to adjacent site traffic pattern, as described in subclause 4.2, a MS SPRing gives a better utilisation of the total traffic capacity of the ring compared to the MS DPRing.

6.2.2 Network objectives

Number of nodes: the maximum number of nodes in an MS SPRing shall be 16 (requiring four bits for an address). This may be less due to the distribution of traffic.

The uniform traffic pattern has the most significant impact on the number of nodes for full connectivity. The maximum number of nodes for full connectivity is shown in table 1. The derivation of these values and values for other traffic patterns is given in annex A.

Table 1: MS SPRing bit rate, granularity and number of nodes for full connectivity with uniform traffic

Bit rate (S)	STM-4	STM-16
Granularity (G)	AU-4	AU-4
S/G	2	8
Number of nodes	3	7

Switch time: for MS SPRings, with no secondary or secondary traffic and no previous switch requests, and less than 1 200 km of fibre the protection switch time shall be less than 50 ms.

Protection switch time excludes the detection time necessary to initiate the protection switch.

Secondary traffic: for MS SPRings, access to the protection trails may be provided as an option to accommodate secondary, low priority traffic.

LO VC access: MS SPRings, in addition to AU-4 access, may provide access to LO VCs in order that they can be added, dropped or passed through.

In the case where squelching of the LO VCs based directly on information in the MS trails is used, this may not be compliant with ITU-T Recommendation G.803 [3]: This requires further study.

Extent of protection: the ring shall restore all of the restorable traffic from a single point failure, including a nodal failure, a section failure and an optical component failure.

The ring protection shall recover from multiple failures in a predictable manner, which may result in multiple segments of the rings.

Switching types: the type of protection switching shall be dual ended.

APS protocol: an APS signalling protocol is required to co-ordinate the switch and bridge operations between the nodes adjacent to a failure.

Operation modes: the mode of protection switching operation shall be revertive.

Physical size of ring: in order to meet the required protection switching time, the fibre circumference of a 16 node MS SPRing should be less than 1 200 km.

Network transfer delay may impose an additional limitation on the physical size of a ring assuming the network does not use echo cancellers. Path availability may also impose a limit on the physical size of a ring.

Upgradability: it shall be possible to add and delete nodes from a ring, or upgrade the capacity of a ring or an optical section.

Manual control: external commands shall be provided for manual control of protection switching by the operations systems or the craftpersons. These commands include:

Clear: to remove externally initiated request and wait to restore;
Lockout of working channels: to stop working channels access to the protection channels;
Forced switch: to switch working channels to protection channels, unless an equal or higher priority request or signal failure condition exists on the protection channels;
Manual switch: to switch working channels to protection channels, unless an equal or higher priority bridge request exists on the ring;
Exerciser: to perform protection switching without completing the bridge and switch.

Synchronization distribution: distribution of synchronization may be independent of the ring. Thus protection of synchronization trails should be considered and should be independent of traffic protection. The general principles defined in ITU-T Recommendation G.803 [3] shall be applied. If the synchronization signal is distributed around the ring, timing loops should be prevented.

6.2.3 Network operation

A two-fibre MS SPRing is a ring in which one fibre carries both the working and protection traffic in one (clockwise) direction, and the other fibre carries both the working and protection traffic in the opposite (anti-clockwise) direction.

The capacity of each fibre is divided equally between the working capacity for transporting the working traffic and the protection capacity for transporting the protection traffic.

Figure 5 shows the operation of a two-fibre MS SPRing under normal conditions with the working traffic between nodes A and B, and between nodes A and C.

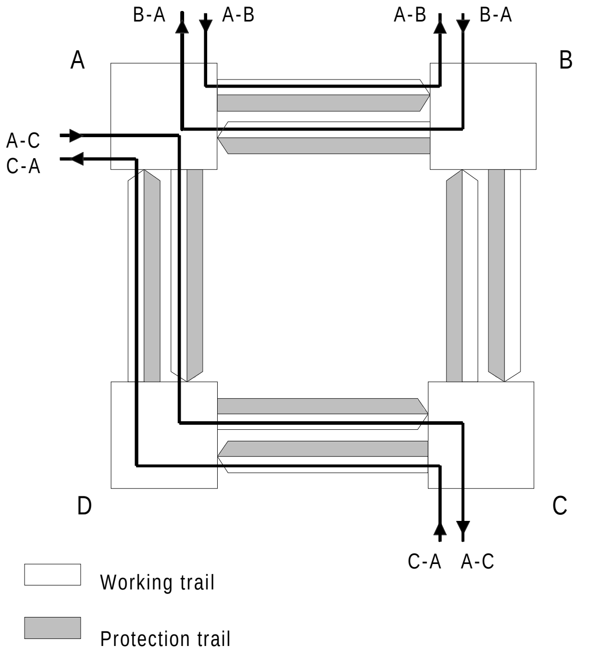


Figure 5: Two-fibre MS SPRing (normal conditions)

In the event of failure conditions, the working traffic carried in the direction towards the failure is looped (i.e. bridged) at a node adjacent to the failure, onto the protection trail in the opposite direction away from the failure. This is head end bridge.

The traffic is recovered at the other node adjacent to the failure by looping (i.e. switching) the protection traffic carried in the direction towards the failure onto the working trail in the opposite direction away from the failure. This is the tail end switch.

6.2.3.1 Single point failure

A section or link failure and an optical component failure are examples of single point failure. They give rise to either an unidirectional link failure or a bi-directional link failure.

Figure 6 illustrates a bi-directional link failure between node A and C. The bi-directional working traffic is recovered by the nodes A and D. Node D performs tail end switch and node A performs a head end bridge in order to recover A to C communication. C to A direction is recovered with a tail end switch in node A and a head end bridge in node D.

In case of an unidirectional failure as shared rings have dual ended switching the final result is exactly the same as in figure 6.

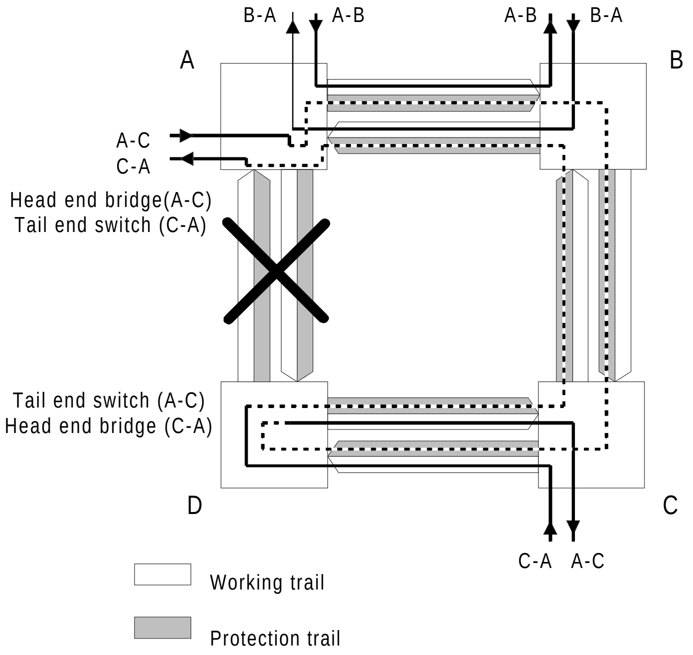


Figure 6: Two-fibre MS SPRing (bi-directional link failure)

6.2.3.2 Multiple failures

Single point failure occurring at more than one physical location in a ring is considered as multiple failures. These failures are either link failures (single point failures) or nodal failure, or combination of them.

The operation of single point failure described in subclause 6.2.3.1 and nodal failure described in subclause 6.2.3.3 applies. Multiple failures may result in ring segmentation.

6.2.3.3 Nodal Failure

A node failure can be considered as a bi-directional link failure occurring on both sides of the node.

Figure 7 illustrates a nodal failure at node D. The bi-directional working traffic between nodes A and C is recovered by the nodes A and C performing both a head end bridge and a tail end switch.

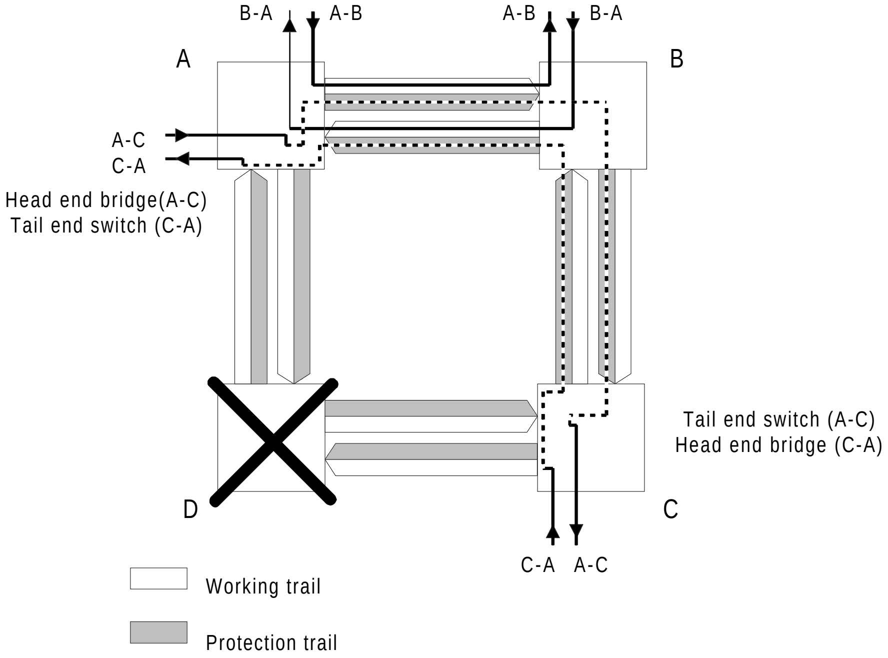
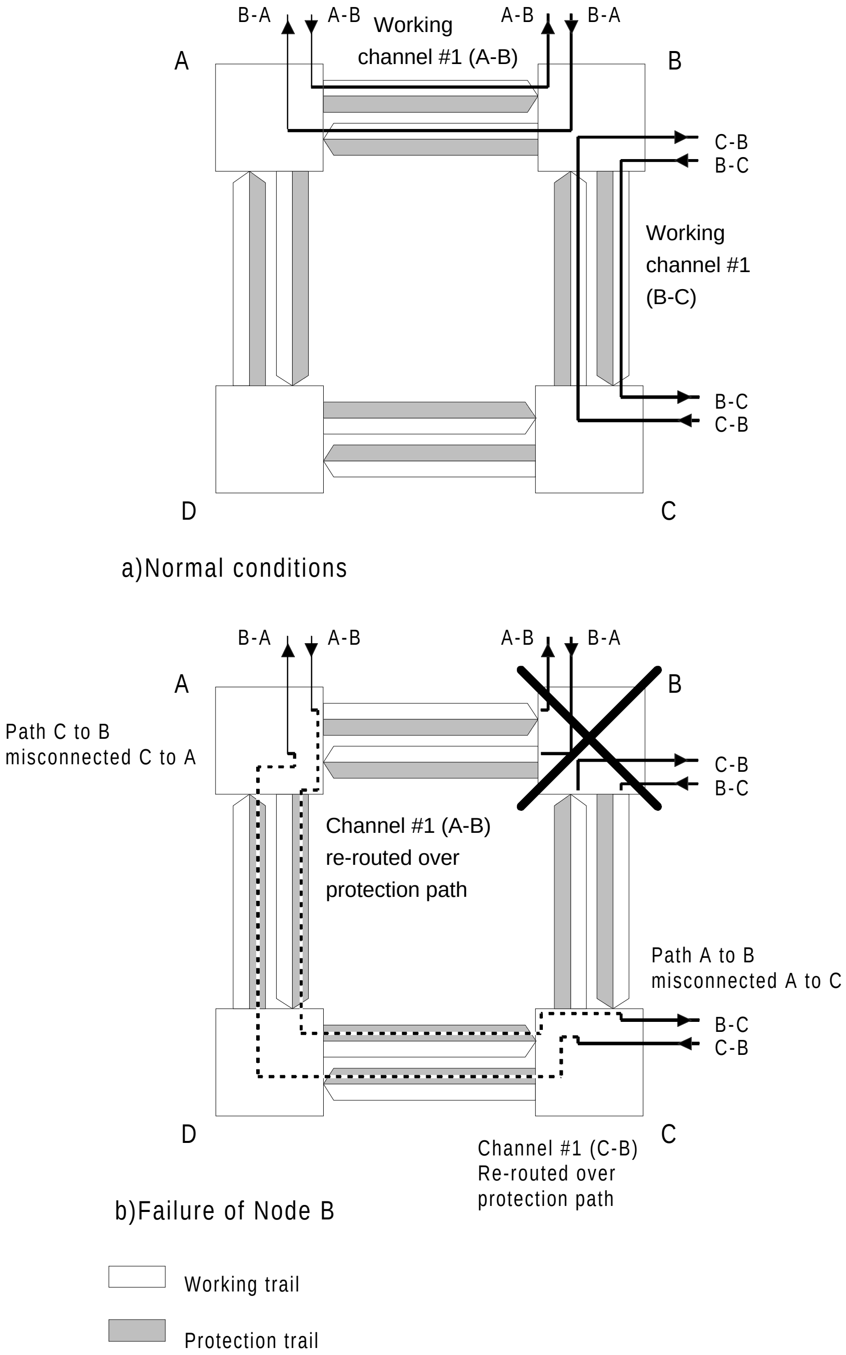


Figure 7: Two-fibre MS SPRing (nodal failure)

6.2.4 Traffic misconnection

Traffic misconnection may occur, under nodal or multiple failures, when working traffic originated and terminated from a failed or isolated node is routed onto the protection trail and terminated at a different node from which it was originally intended.

Figure 8 gives an example of traffic misconnection when node B fails. It shows that the working traffic between nodes B and C and that between nodes B and A are both assigned to the same working channel or timeslot #1, resulting in a misconnection between nodes C and A.



a)Normal conditions

b)Failure of Node B

Figure 8: An example of traffic misconnection

Squelching of mis-connected traffic at the AU level should be performed at the switching nodes by inserting AU-AIS for the mis-connected AU traffic which does not have LO VC access. For rings using LO VC access, squelching locations are under study.

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

There are two options for handling the problems caused by a node that allows interconnectivity between any ports:

- the mis-routed traffic is squelched;
- the mis-routed traffic is re-routed.

The re-routeing method of handling mis-routed traffic would increase the complexity and size of information (e.g. ring maps) required by every ring node and the APS algorithm. The choice between the two methods depends on the trade off between the flexibility of time slot interchange of pass through traffic and the complexity of APS algorithm management.

6.2.5 Secondary traffic

This secondary traffic is not itself protected. In the event of a protection switch all the secondary traffic in the protection trail is removed, i.e. squelched by inserting path AIS.

6.2.6 LO VC access

In an STM-4 ring with VC-4 access, depending on the traffic pattern, the maximum number of nodes based on the assumption that all paths are fully protected and simultaneous access is required, is greater than or equal to 3. This is described in subclause 6.2.2 and shown in table 1. LO VC access at each node may be required to provide greater flexibility of capacity distribution and would allow a greater number of nodes.

In an STM-16 ring with VC-4 access, depending on the traffic pattern, the maximum number of nodes based on the assumption that all paths are fully protected and simultaneous access is required, is greater than or equal to 7. This is also described in subclause 6.2.2 and shown in table 1. In this case LO VC access may be required to provide greater flexibility of capacity distribution.

6.2.7 Functional model

All the examples are based on STM-4 rings to simplify the figures. In these models, the possible lower order VC access is not shown.

Figures 9 to 11 deal with the functional models for a two-fibre MS SPRing. Figure 9 shows the node in the normal working condition, while figures 10 and 11 show the reconfiguration of the node in the case of a failure on the east side and west side, respectively.

Figure 12 shows an example of a two-fibre MS SPRing in the normal state with secondary traffic including the Multiplex Section Protection Connection (MSPC) matrix connections. Figure 13 shows the MSPC connections when there is a fault on the east side and Figure 14 shows the MSPC connection in the pass through state.

6.2.8 Protection interworking

The interworking scenarios between the MS SPRings and other schemes are described in TS 101 010 [1].

6.2.9 Switch initiation criteria

MS SPRing switch requests can be initiated manually. They are also initiated based on Loss Of Signal (LOS), Loss Of Frame (LOF), Multiplex Section - Alarm Indication Signal (MS-AIS) and error performance.

Details of the switch initiation criteria for the MS SPRings are described in ETS 300 746 [2].

6.2.10 APS protocol

Details of the APS protocol and operation for the MS SPRings are described in ETS 300 746 [2].

6.2.11 MS SPRing with enhanced protection selectivity

In a number of applications it can be beneficial to increase the protection selectivity of the MS SPRing.

In such applications it is desirable to be able to interchange protected channels for unprotected channels.

Below three applications for such a feature are given:

i) in some applications it is not needed to protect the traffic in the SDH transport layers;

ii) in many applications end-to-end protection will be used for premium leased lines. If this traffic will pass an MS SPRing then the traffic has double protection. This is not always needed. The option to carry this traffic on an MS SPRing without additional protection, will further increase the efficiency;

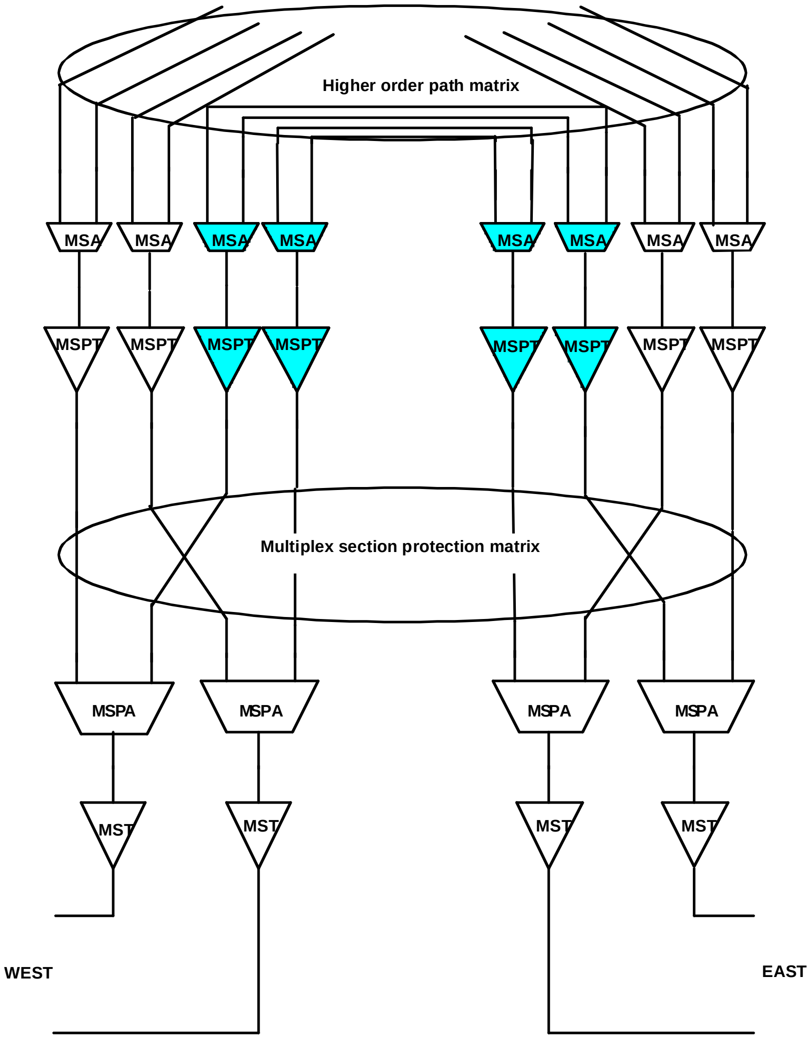
iii) if there are STM-16 rings with 2 Mbit/s access and part of the traffic is local for that ring, then it can be attractive to reserve some VC4s for the local traffic and apply LO (S)NC protection for that traffic. The possibility to exclude some VC4s from the MS SPRing operation offers advantages.

It is proposed to enhance the description of the MS SPRing operation in this present document with the option to exclude some VC4 ring channels from the MS SPRing operation. This can be done effectively by defining non-pre-emptible unprotected channels.

The choice per VC4 shall be made on a ring basis and per VC pair. If a VC4 working channel will not be part of the MS SPRing operation, then this is also the case for its corresponding protection channel, and for these two channels it is true for the whole ring.

This feature will make it possible to interchange protected channels for unprotected channels on a VC4 ring pair basis. This feature will not have any impact on the MS SPRing APS protocol, it is a matter of provisioning of the ring nodes.

This is for further study.

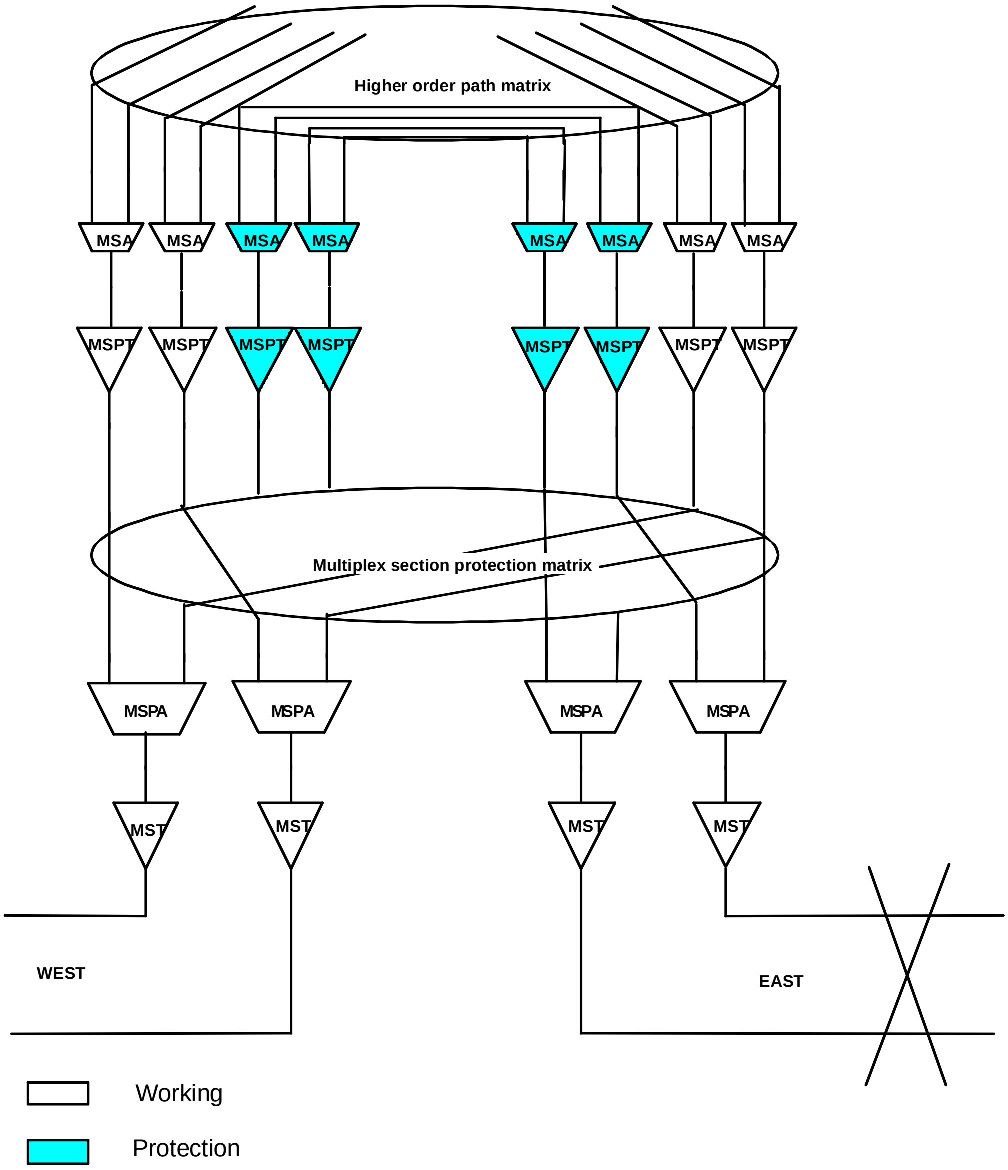


□ Working

🟦 Protection

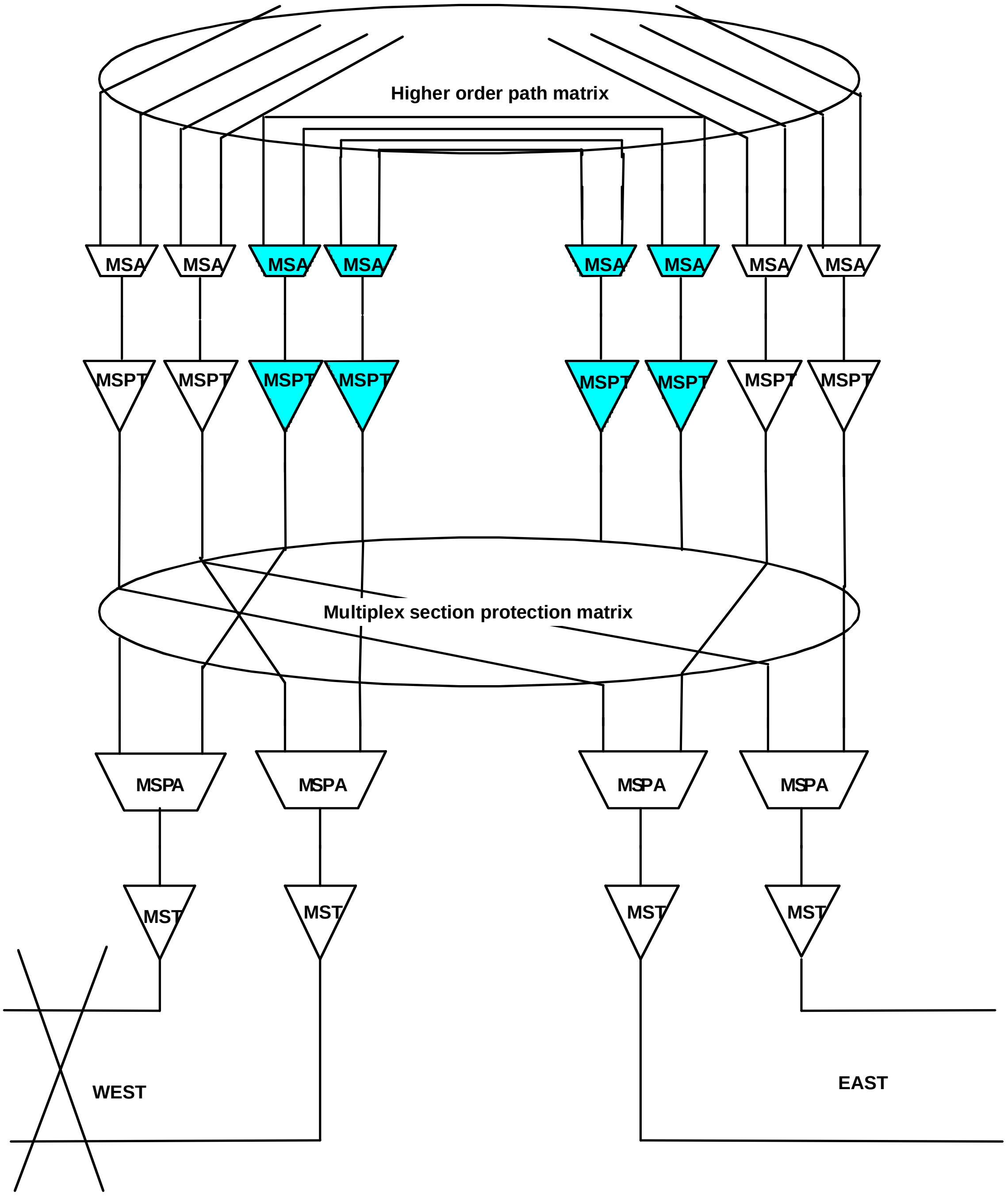
MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 9: Node of a two-fibre MS SPRing



MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 10: Node of a two-fibre MS SPRing with a fault on the east side

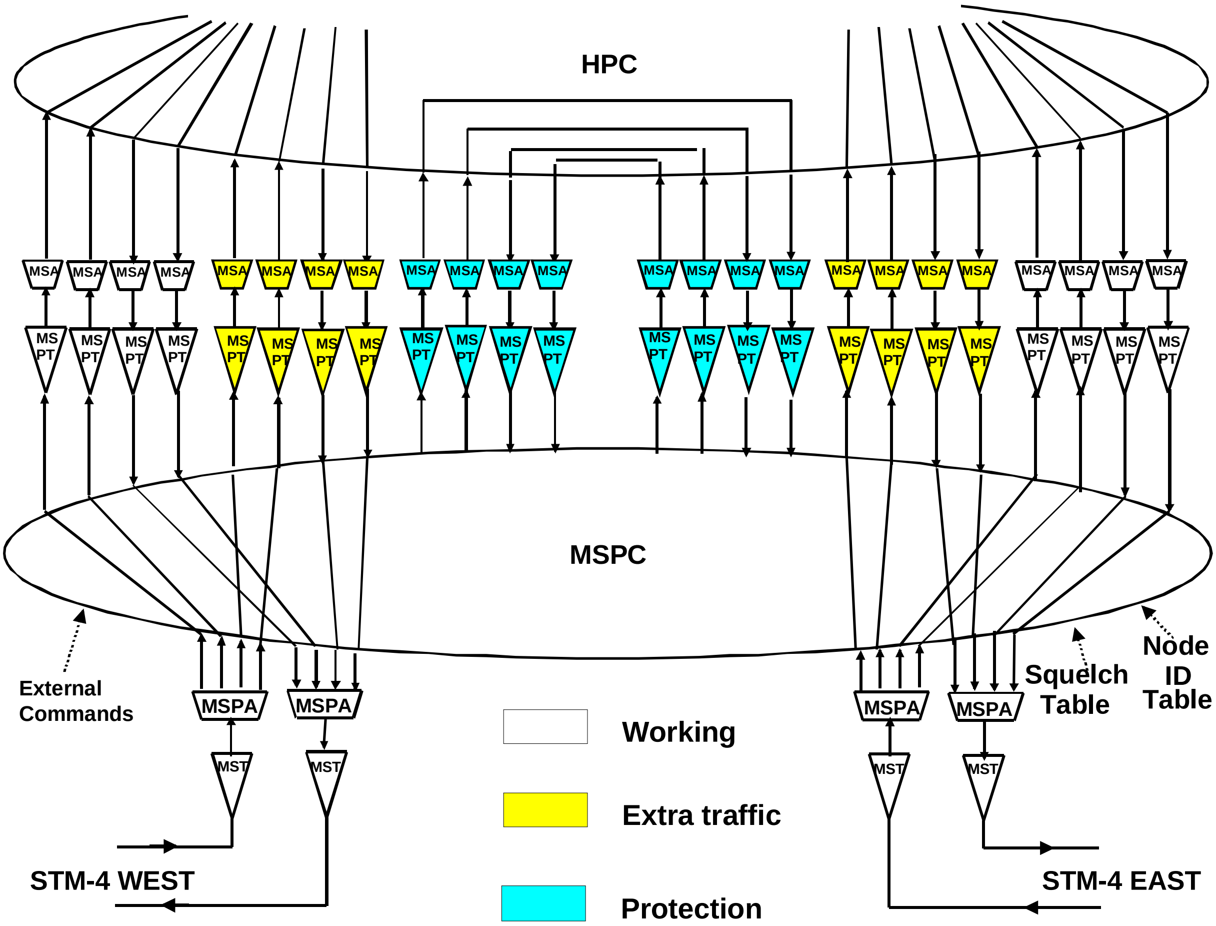


□ Working

🟦 Protection

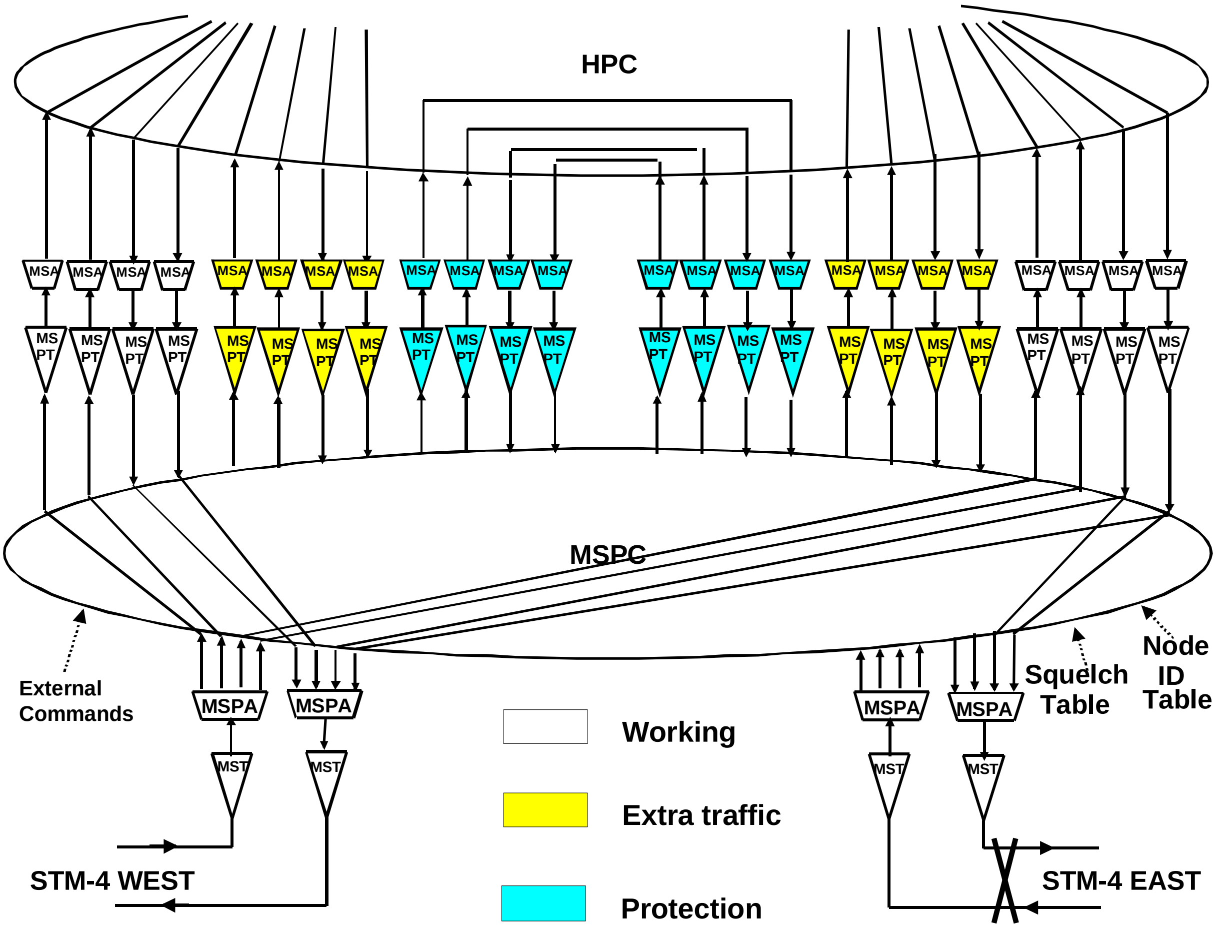
MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 11: Node of a two-fibre MS SPRing with a fault on the west side



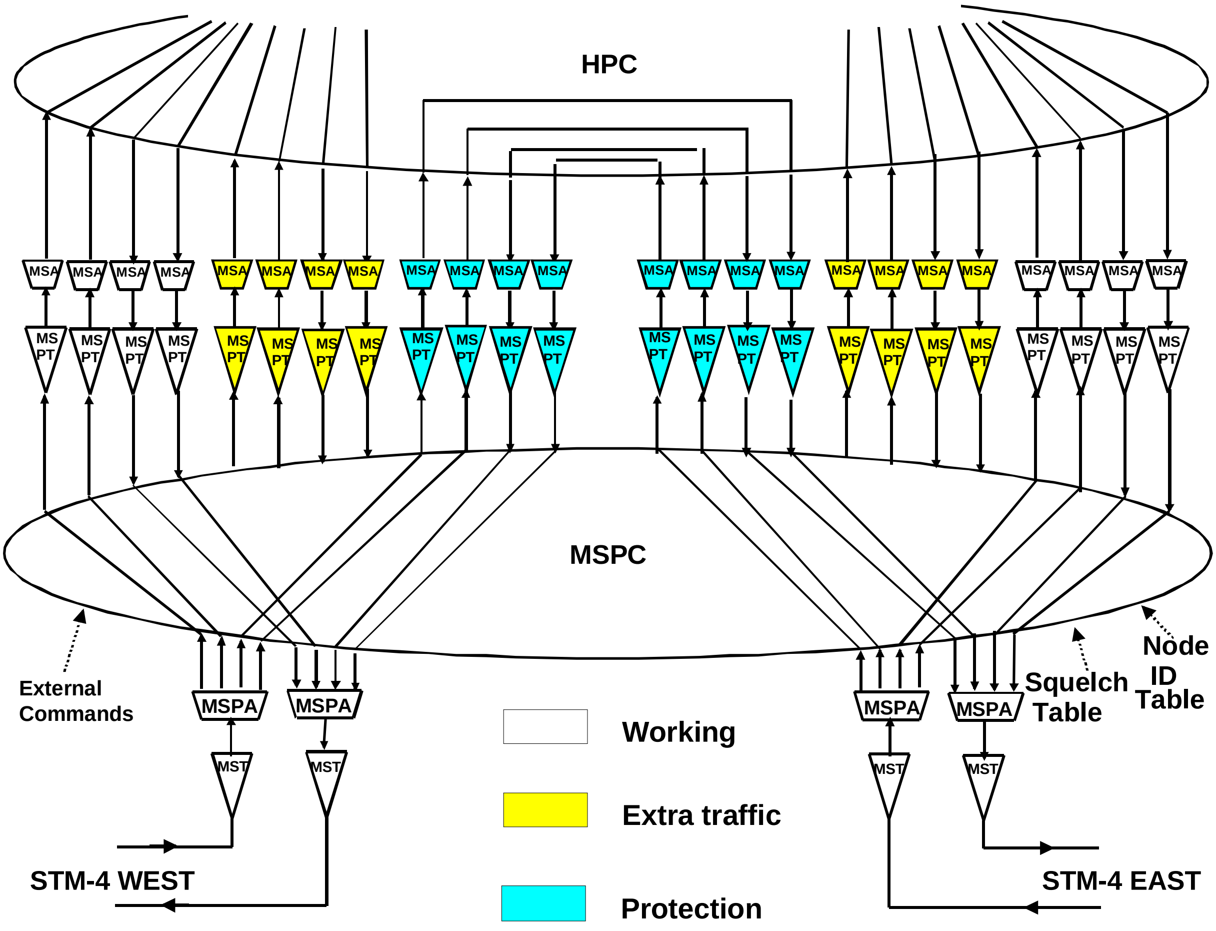
HPC	Higher order Path Connection
MSA	Multiplex Section Adaptation
MSPA	Multiplex Section Protection Adaptation
MSPC	Multiplex Section Protection Connection
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination

Figure 12: Functional model for a two-fibre MS SPRing - normal state with secondary traffic



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

Figure 13: Functional model for a two-fibre MS SPRing - failure on the east side



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

Figure 14: Functional model for a two-fibre MS SPRing - pass-through state

6.3 Four-fibre MS SPRing

The four-fibre ring is for further study.

6.4 Multiplex Section Dedicated Protection Ring (MS DPRing)

6.4.1 Network architecture

The normal mode of operation for a MS DPRing is to use diverse routeing, e.g. the working traffic is transmitted in one direction (e.g. clockwise) only and the protection traffic is transmitted in the opposite direction (e.g. anti-clockwise). In functional modelling of a transport network in ITU-T Recommendation G.803 [3], this is defined as unidirectional connections. In this case the working MS trail is unidirectional or can be regarded as one half of a bi-directional MS trail, the other half forming the unidirectional protection MS trail. If a failure occurs in the ring, the unidirectional working MS trail is replaced by a unidirectional protection MS trail.

It is also possible to operate the ring with uniform routeing and/or unprotected traffic. It should be noted that protected uniform routeing makes less efficient use of the ring capacity.

Nodal failure conditions result in loopback of traffic to the originating node.

It is a dedicated MS protection ring because it provides one dedicated protection entity for each working entity.

6.4.2 Network objectives

The objective is to provide a simple protection scheme e.g. a scheme that is compatible with the linear MS protection scheme. A consequence is that, for example, secondary traffic capacity is not foreseen.

Number of nodes: the uniform traffic pattern has the most significant impact on the number of nodes for full connectivity. The maximum number of nodes for full connectivity is shown in table 2. The derivation of these values and values for other traffic patterns is given in annex A.

Table 2: MS DPRing size, granularity and number of nodes for full connectivity with uniform traffic

Size (S)	STM-1	STM-4		STM-16
Granularity (G)	TU-12	AU-4	TU-12	AU-4
S/G	63	4	252	16
Number of nodes	11	3	22	6

Switch time: for MS DPRings and no previous switch requests, and less than 1 200 km of fibre the protection switch time shall be less than 50 ms.

Protection switch time excludes the detection time necessary to initiate the protection switch.

Secondary traffic: there is currently no provision for secondary traffic in MS DPRings. 1:1 operation is for further study.

LO VC access: MS DPRings, in addition to AU-4 access, shall provide access to LO VCs in order that they can be added, dropped or passed through.

Extent of protection: the ring shall restore all of the restorable traffic from a single point failure, including a nodal failure, a section failure and an optical component failure.

The ring protection shall recover from multiple failures in a predictable manner, which may result in multiple segments of the rings.

Switching types: the type of protection switching shall be dual ended.

APS protocol: an APS signalling protocol is required to co-ordinate the switch and bridge operations between the nodes adjacent to a failure.

Operation modes: the mode of protection switching operation shall be revertive.

Physical size of ring: in order to meet the required protection switching time, the fibre circumference of an MS DPRing should be less than 1 200km.

Network transfer delay may impose an additional limitation on the physical size of a ring assuming the network does not use echo cancellers. Path availability may also impose a limit on the physical size of a ring.

Two or four fibre ring: only two-fibre MS DPRings are considered in this report. Four-fibre rings are for further study.

Upgradability: it shall be possible to add and delete nodes from a ring, or upgrade the capacity of a ring or an optical section.

Manual control: external commands shall be provided for manual control of protection switching by the operations systems or the craftpersons. These commands include:

Clear: to remove externally initiated request;
Lockout of working channels: to stop working channels access to the protection channels;
Lockout of protection: to disable protection switching;
Forced switch: to switch working channels to protection channels, unless an equal or higher priority request or signal failure condition exists on the protection channels;
Manual switch: as Forced Switch, except that the protection channels are fault free;
Exerciser: to perform protection switching without completing the bridge and switch.

Synchronization distribution: not applicable.

6.4.3 Network operation

In a ring, traffic has two routes in order to go from a point to another. As an example, traffic is carried by clockwise direction of a VC, while the counter clockwise direction of the VC forms a logical ring for protection purposes. This logical ring is realized with permanent pass through in intermediate nodes. In case of failure, traffic is looped back on protection.

There are two requirements:

- Payload is looped back upon section alarm;
- VC are unidirectional (see ITU-T Recommendation G.783 [6] §2.6 and 2.10).

6.4.3.1 Single point failure

When there are section alarms, the section's payload is looped back, resulting in traffic transported by the VCs being re-routed on the protection ring.

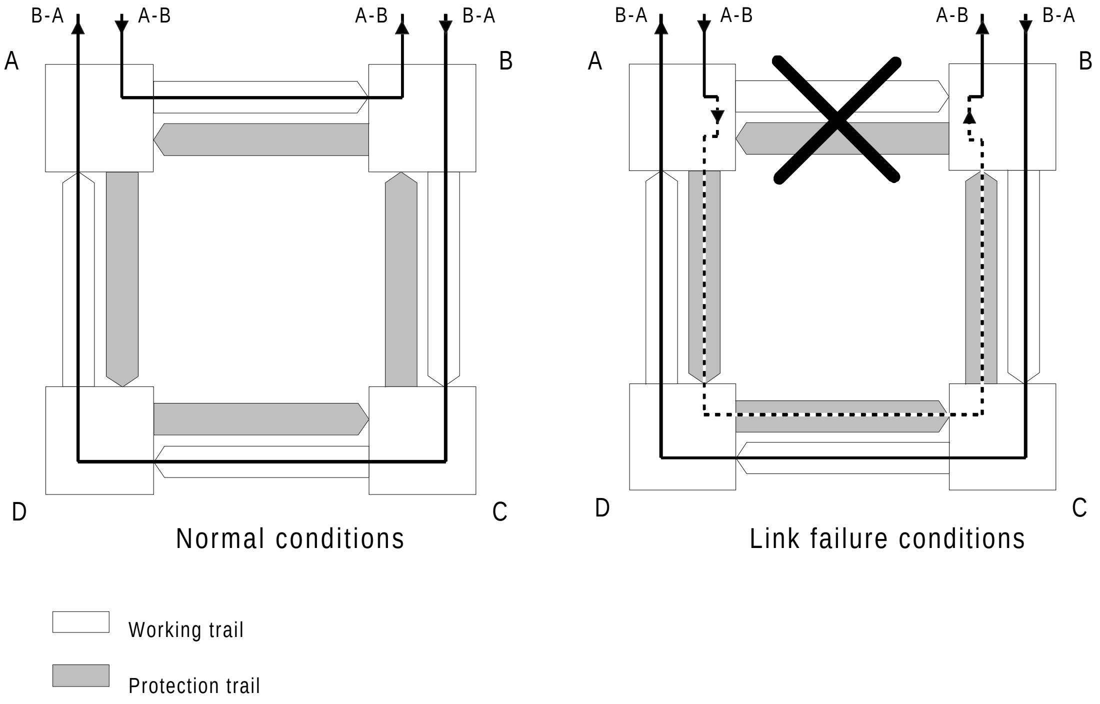


Figure 15: Two-fibre MS DPRing

In figure 15, under normal conditions, VC carries traffic in clockwise direction. In case of a link failure, traffic is re-routed via anti-clockwise direction of the VC. The whole payload is looped back at once.

6.4.3.2 Multiple failures

In case of multiple failure shown in figure 16, there will be two or more segments. These failures may be node or link failures.

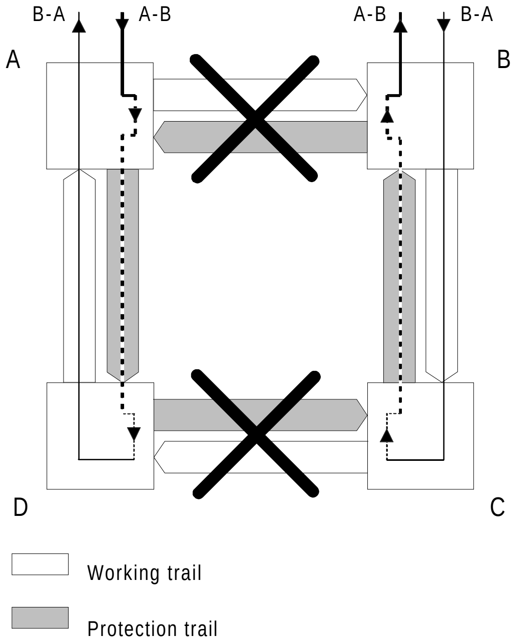


Figure 16: Two-fibre MS DPRing (multiple failures)

6.4.3.3 Nodal failure

When there is a nodal failure, paths which were terminated at this node are looped on themselves, source to sink. When trace identifier mismatch is detected (which may be outside the MS DPRing), AIS is inserted.

6.4.4 Traffic mis-connections

There is no traffic misconnection between two different subscribers with 1+1 dedicated protection mechanism.

6.4.5 Secondary traffic

There is no secondary traffic with this 1+1 dedicated protection mechanism.

6.4.6 LO VC access

The mechanism works with LO and HO accesses.

6.4.7 Functional model

The following functional models are based on ITU Recommendation G.803 [3]. In these models the possibility of lower order VC access is not shown.

Figure 17 shows the generic functional model for MS DPRing in normal conditions. On this example, working direction of the path is running from west to east.

Figure 18 shows the generic functional model for MS DPRing after a failure on the west side.

Figure 19 shows the generic functional model for MS DPRing after a failure on the east side.

Figures 20, 21 and 22 show examples of the functional models for a two fibre, STM-4 MS DPRing. Figure 17 shows the node in the normal working condition, while figures 18 and 19 show the reconfiguration of the node in the case of a failure on the east side and west side, respectively.

6.4.8 Protection interworking

The interworking scenarios between MS DPRings and other schemes are described in TS 101 010 [1].

6.4.9 Switch initiation criteria

MS DPRing switch requests can be initiated manually. They are also initiated based on LOS, LOF, MS-AIS and error performance.

Details of the switch initiation criteria for MS DPRings are described in ETS 300 746 [2].

6.4.10 APS protocol

Details of the APS protocol and operation for the MS DPRings are described in ETS 300 746 [2].

6.4.11 Uniform routed connection in MS DPRing architecture

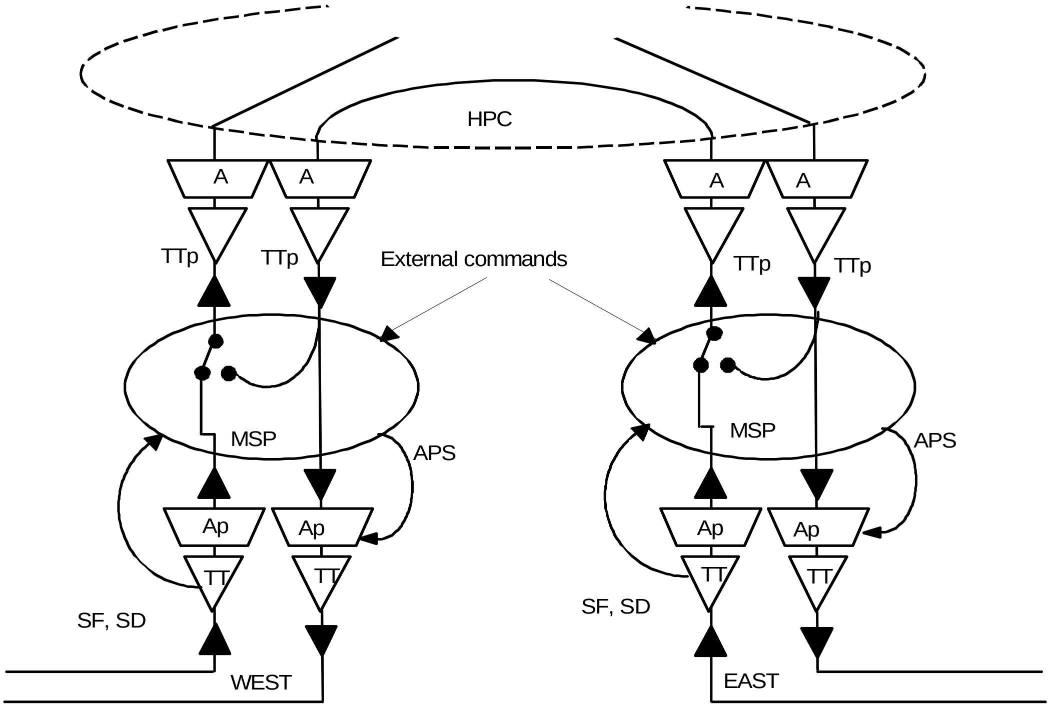
For some applications, uniform routeing of a bi-directional connection may be a requirement (e.g. equal transmission delay). MS DPRing can support this type of routeing.

In this case two working VCs are necessary, e.g. VC#i in one direction and VC#j in the opposite direction.

If a failure occurs, a loopback is activated on each node where the failure is detected on a VC by VC basis. In this way the MS DPRing topology can ensure service continuity after a failure.

6.4.12 Unprotected VC in MS DPRing architecture

It is possible to mix protected and unprotected traffic in a MS DPRing. However in this case, if a failure occurs, the unprotected traffic will be looped to the originating node. When trace identifier mismatch is detected (which may be outside the MS DPRing), AIS is inserted.



NOTE: On this example, working direction of the path is running from west to east.

Figure 17: Generic functional model for MS DPRing in normal conditions

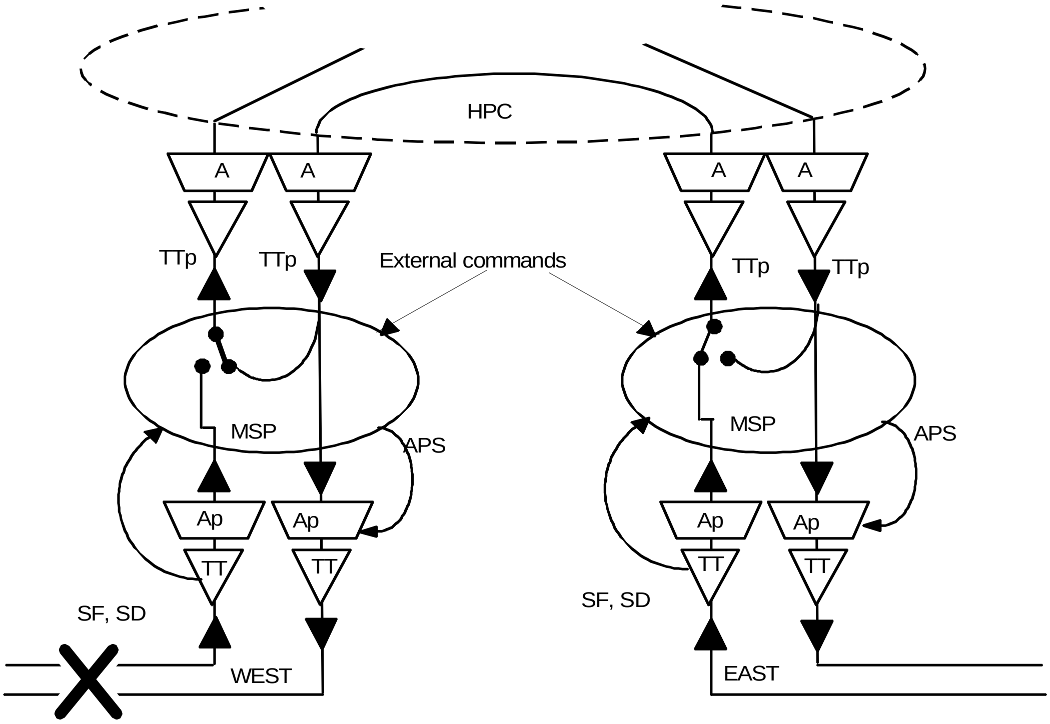


Figure 18: Generic functional model for MS DPRing after a failure on the west side

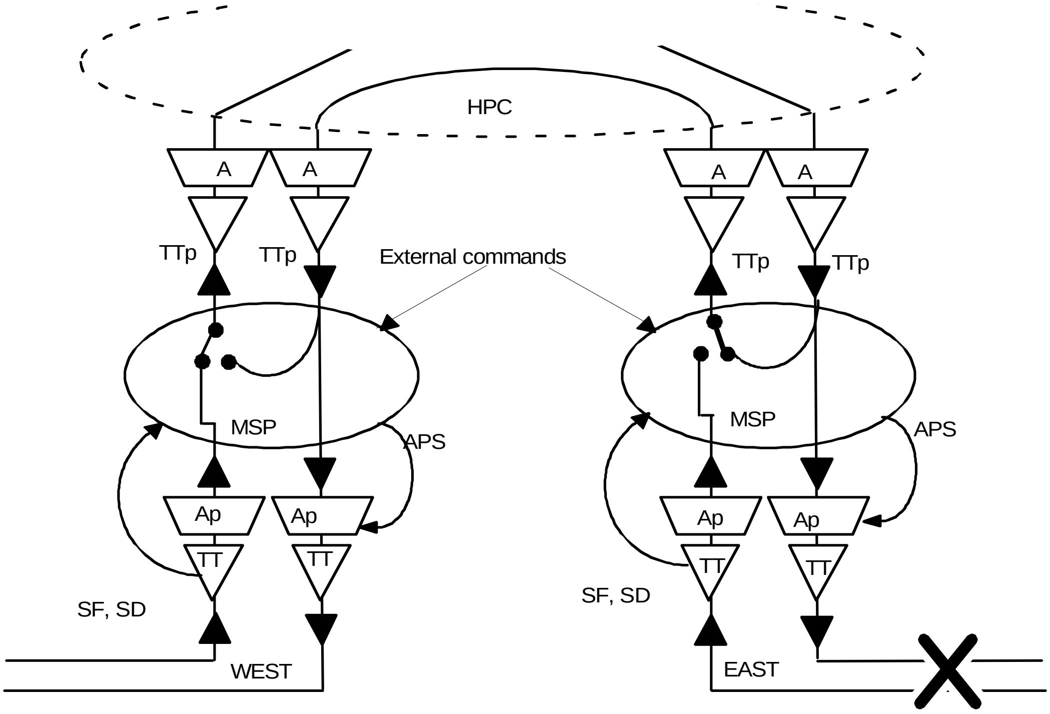
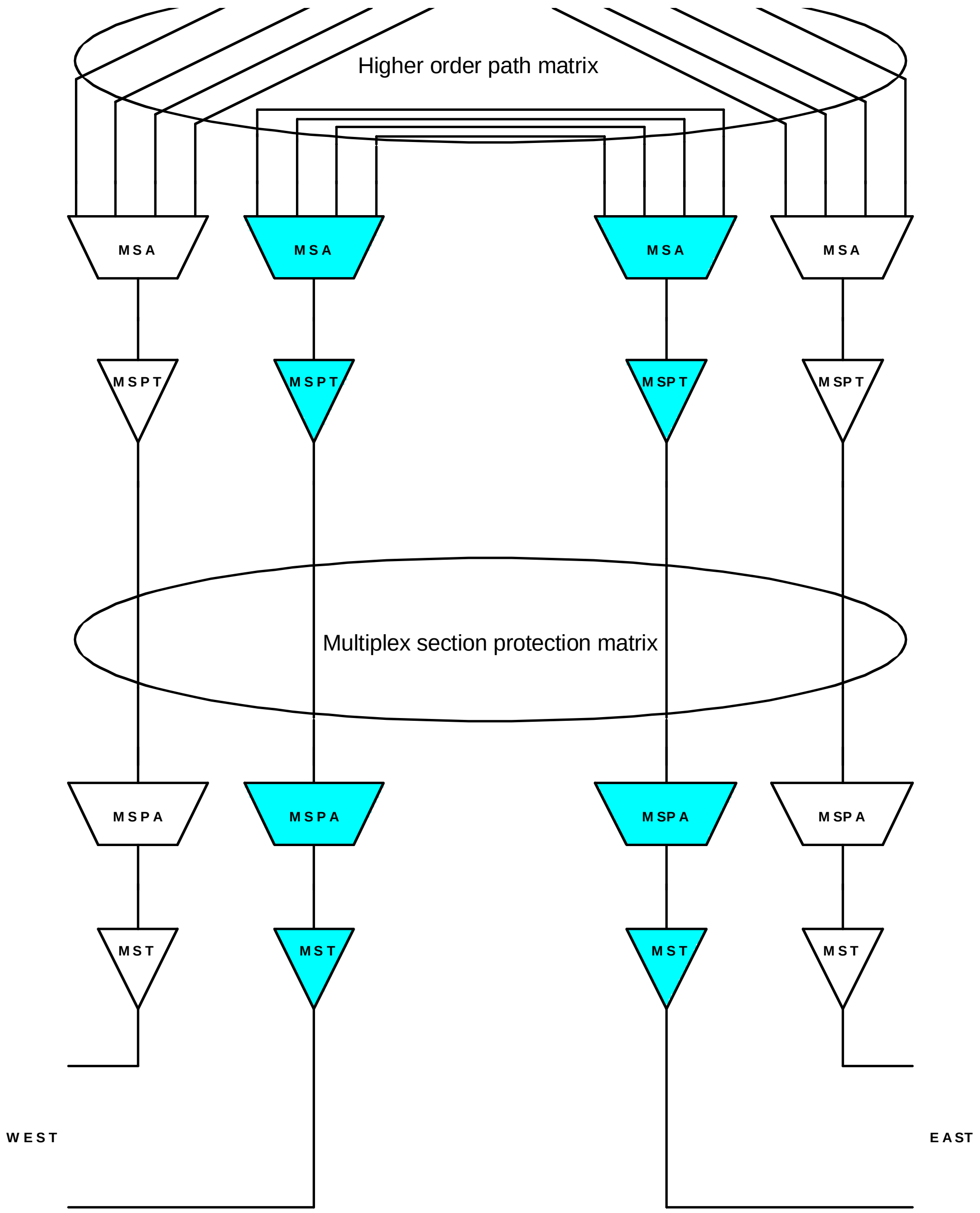


Figure 19: Generic functional model for MS DPRing after a failure on the east side

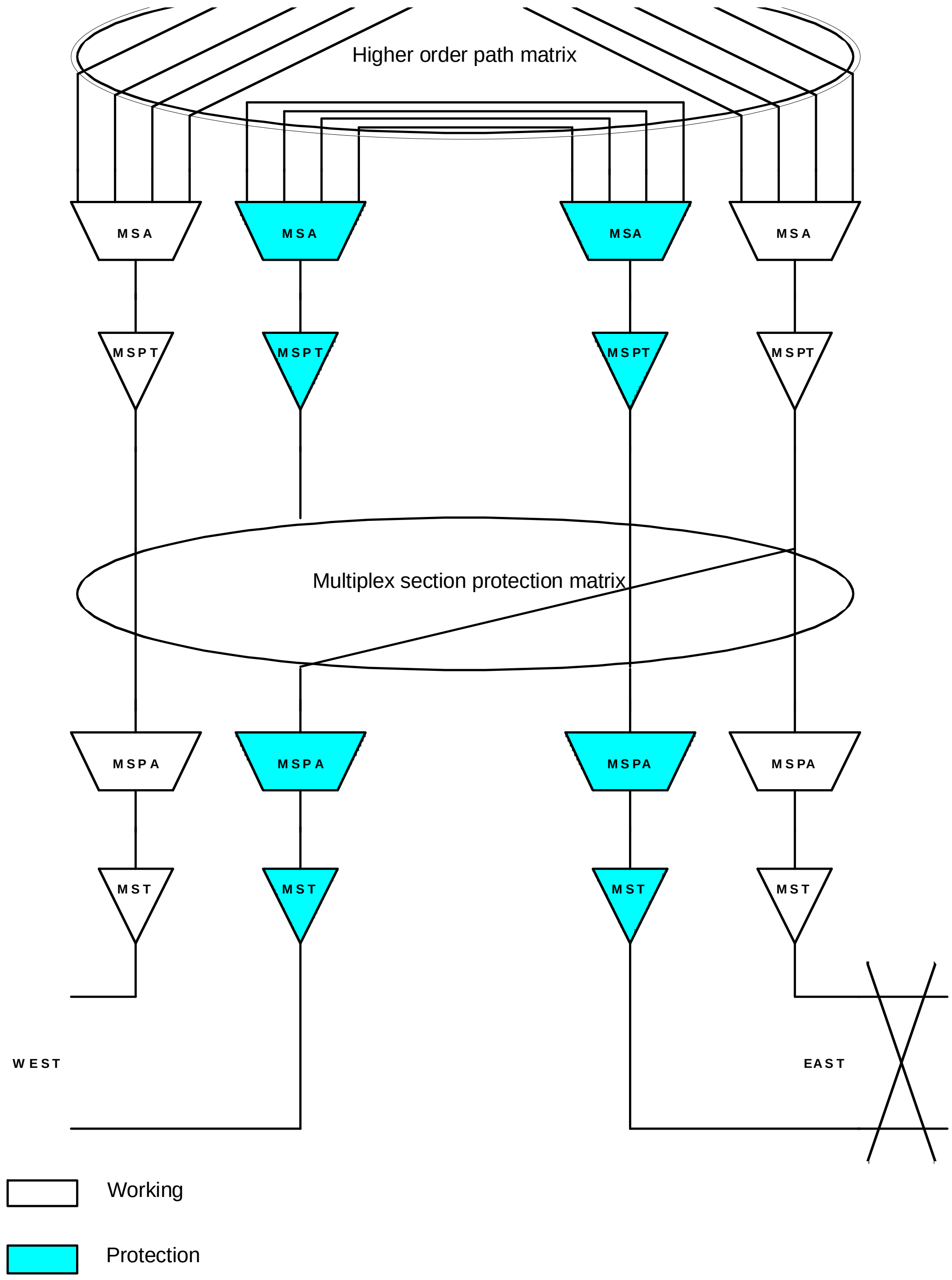


□ Working

🟦 Protection

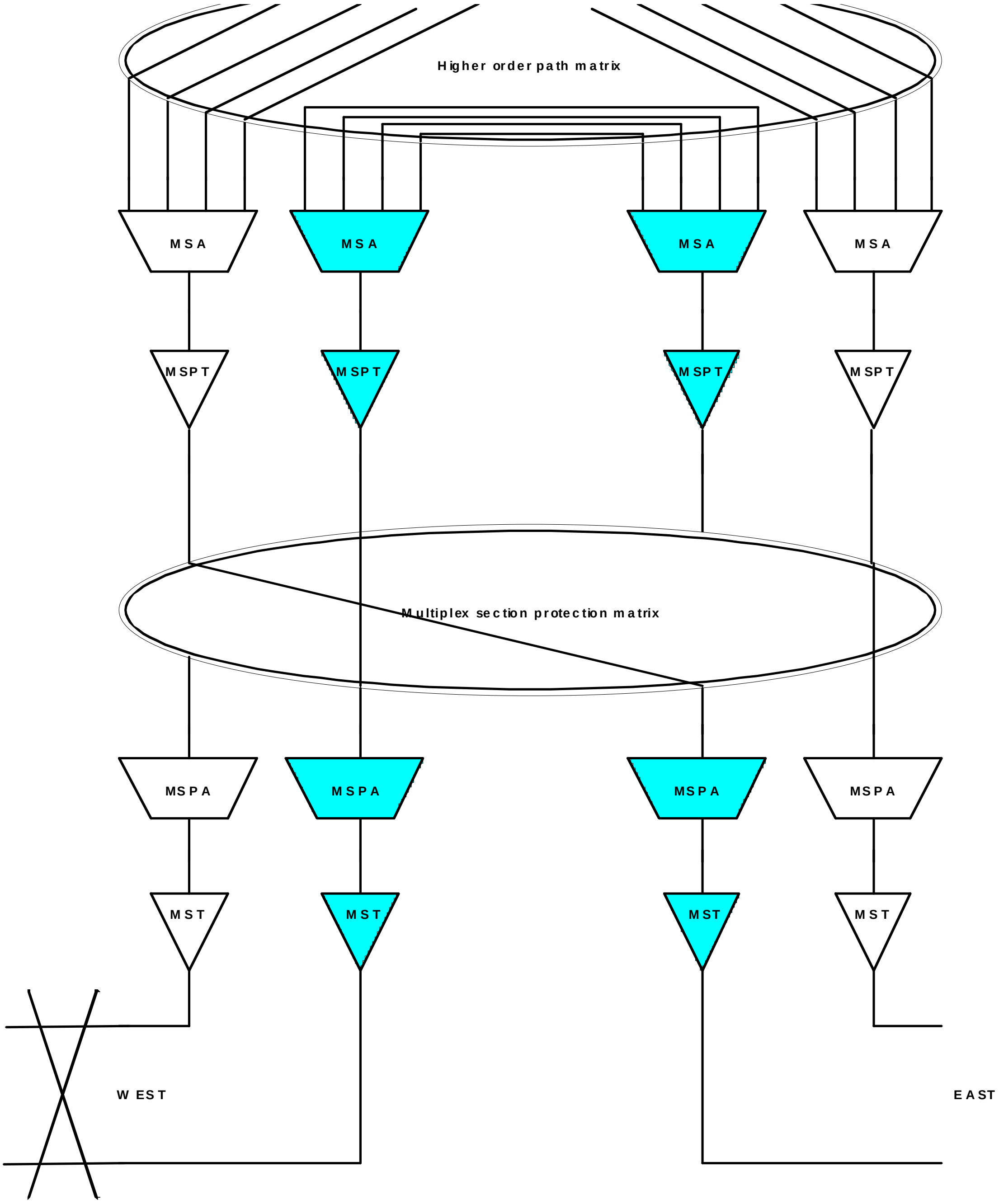
MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 20: Node of a two fibre MS DPRing



MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 21: Node of a two-fibre MS DPRing with a fault on the east side



☐ Working

🟦 Protection

MSA	Multiplex Section Adaptation
MSPT	Multiplex Section Protection Termination
MSPA	Multiplex Section Protection Adaptation
MST	Multiplex Section Termination

Figure 22: Node of a two-fibre MS DPRing with a fault on the west side

7 Linear VC trail protection

7.1 Network architecture

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

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

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

1:n protection schemes where the protection trail is shared between n working trails are for further study.

As VC trail 1:1 dedicated protection is a linear protection mechanism, the working and secondary traffic trail termination functions overlap. In a network application this implies that the working and secondary traffic patterns shall coincide.

VC trail protection does not limit the number of NEs within the network connection.

7.2 Network objectives

The following network objectives apply:

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

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

3) **Hold-off times:** hold-off times are useful for inter-working of protection schemes and these times should be provisionable on an individual VC basis. The failure condition should be continuously monitored for the full duration of the hold-off time before switching occurs. Where digital cross connect equipment is used to carry out the protection switching the switching time may be of the order of seconds. Where a multiplexer equipment is used to implement the switching the switching time will be of the order of 50 ms. The hold-off time should therefore be provisionable from 100 ms to approximately 10 seconds in steps of the order of 100 ms;

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

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

6) **APS protocol and algorithm:** the LO and HO VC trail protection APS protocols should operate in a similar manner for all network applications. The minimum requirement for the protocol is that it can support 1+1 dedicated protection. A 1:1 option to accommodate secondary traffic is desirable and is for further study;

7) **Operation modes:** non-revertive switching is the minimum requirement for 1+1 protection. Requirements for 1:1 and 1:n protection are for further study;

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

9) **Switch initiation criteria:** switch initiation should be based on SF and/or SD indications in harmony with definitions used in ITU-T Recommendation G.783 [6];

10) **Upgradability:** it shall be possible to add and delete nodes from a trail, or upgrade the capacity of a link connection;

11) **Synchronization distribution:** distribution of synchronization may be independent of the sub-network. Thus protection of synchronization trails should be considered and should be independent of traffic protection. The general principles defined in ITU-T Recommendation G.803 [3] shall be applied. If the synchronization signal is distributed around the sub-network, timing loops should be prevented.

7.3 Application architecture

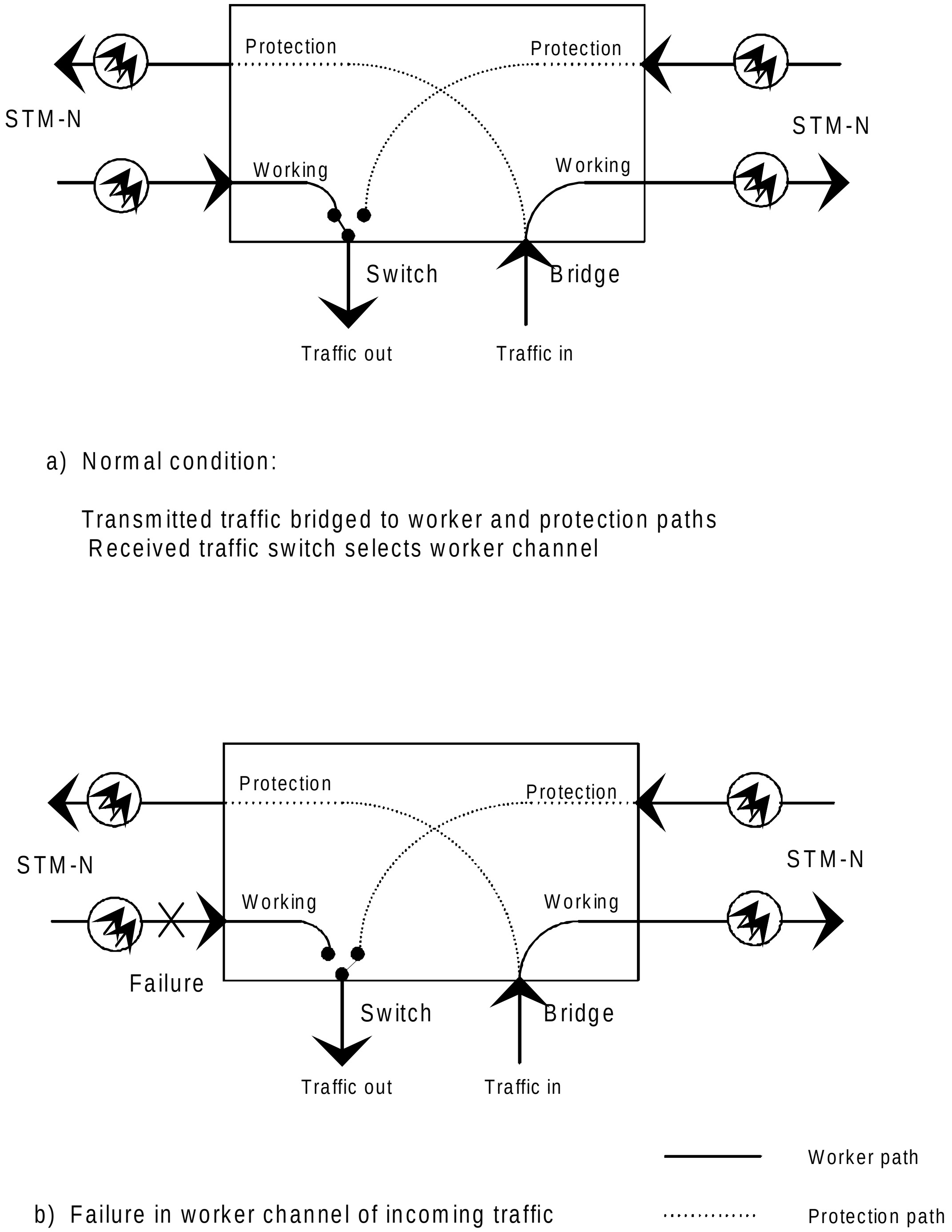
7.3.1 Routeing

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

As noted in the network objectives, the network operator has a choice of uniform or diverse routeing on a per-trail basis. For the simplest case whereby working trails and protection trails are placed on separate routes, the difference in provisioning a node for uniform routeing versus diverse routeing is illustrated for 1+1 protection in figures 23 and 24. For linear VC trail protection, the nodes illustrated contain the termination of the trails involved.

A node using 1+1 uniform routeing under normal operating conditions is shown in figure 23a). A bridge is used to simultaneously transmit signals onto the working and protection trails. The receiver uses a switch to select the working trail under normal operating conditions. Note that the working trails are placed on the same facilities (i.e. the left side of the node). Figure 23b) shows the node when there is a failure in the working trail. In this case, the receiver will detect the loss of signal and will switch to the protection trail.

A node using 1+1 diverse routeing under normal operating conditions is shown in figure 24a). A bridge is used to simultaneously transmit signals onto the working and protection trails. The receiver uses a switch to select the working trail under normal operating conditions. Note that the working trails are placed on different facilities (i.e. one on the left side of the node, the other on the right). Figure 24b) shows the node when there is a failure in the working trail. In this case, the receiver will detect the loss of signal and will switch to the protection trail.



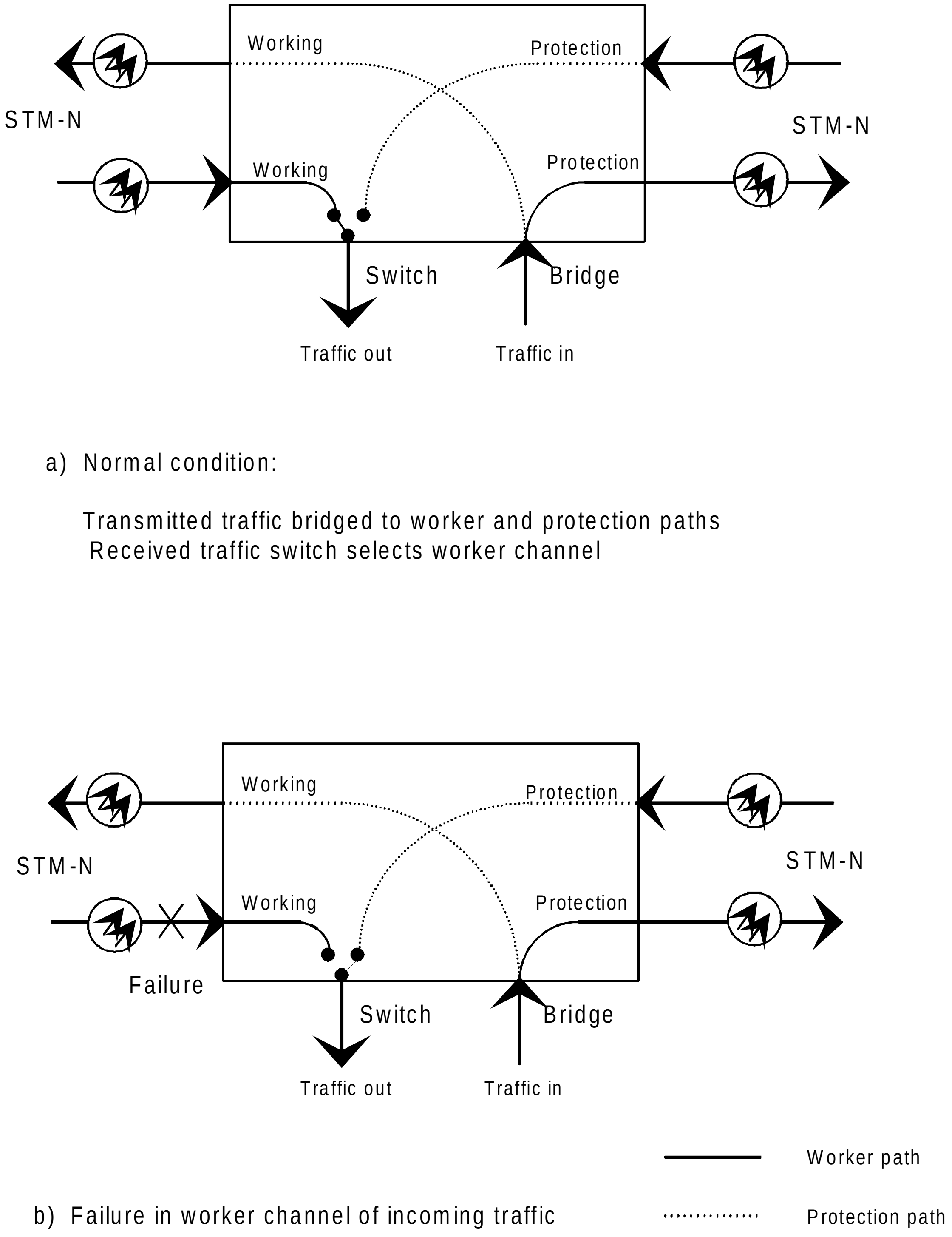
a) Normal condition:

Transmitted traffic bridged to worker and protection paths
Received traffic switch selects worker channel

b) Failure in worker channel of incoming traffic

Receiver switch selects protection path

Figure 23: Node in a unidirectional trail protection network



a) Normal condition:

Transmitted traffic bridged to worker and protection paths
Received traffic switch selects worker channel

b) Failure in worker channel of incoming traffic

Receiver switch selects protection path

Figure 24: Node in a bi-directional trail protection network

7.3.2 1+1 single-ended protection

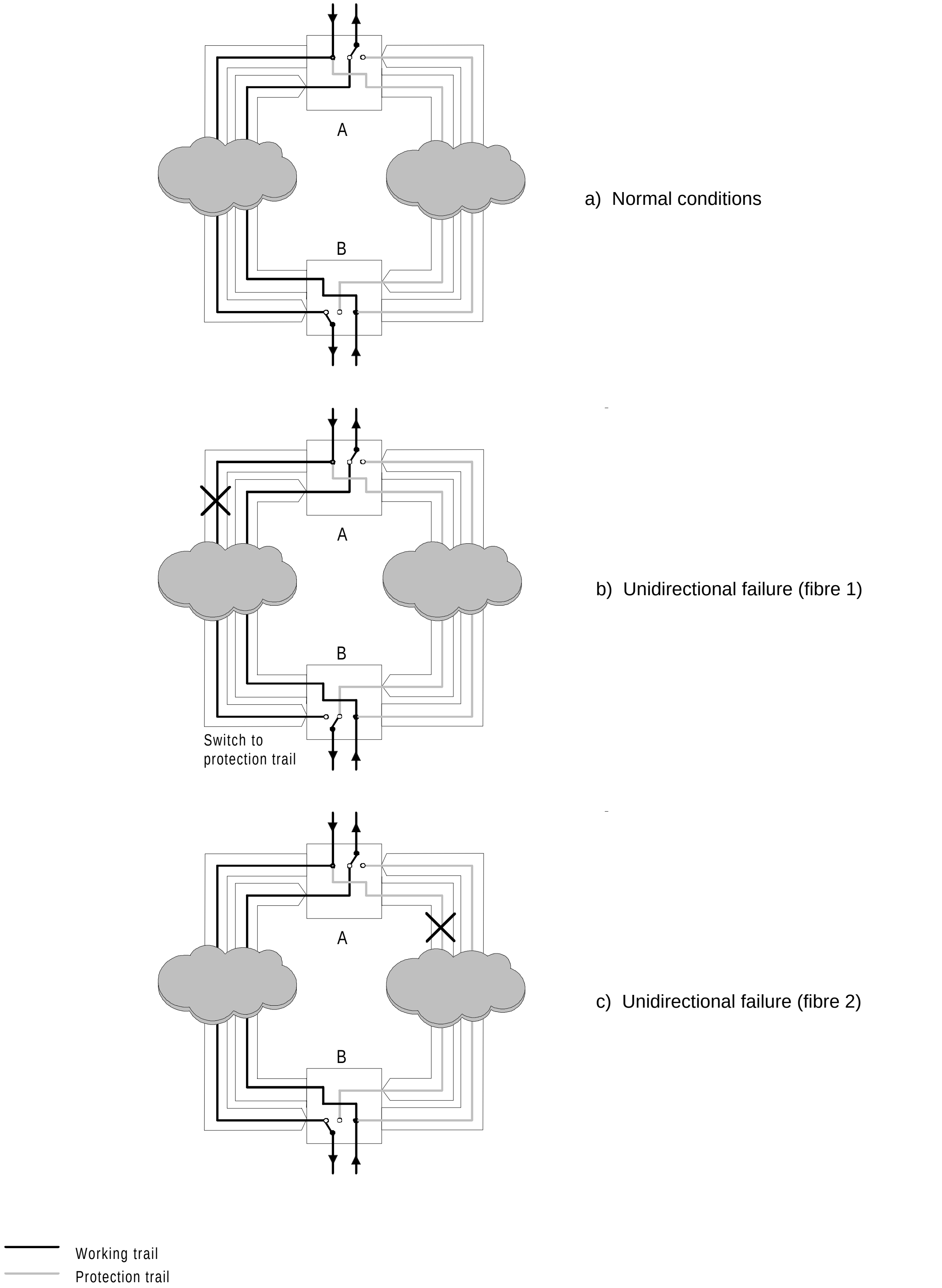
Single-ended protection is illustrated in figure 25 for a uniformly routed 1+1 architecture. It is identical to dual-ended protection, except that for unidirectional failures the unaffected direction of transmission is not switched. Consequently, an APS channel is not required to co-ordinate switching of the unaffected direction of transmission.

Figure 25a) illustrates a 1+1 uniformly routed trail protection network with traffic transmitted between Nodes A and C. Traffic inserted at Node A is transmitted on different trails in two directions to Node C. Under normal operating conditions, the receiver at Node C selects the working traffic. Traffic inserted at Node C is also transmitted in two directions to Node A.

When there is a unidirectional failure on the working trail, as shown in either Figure 25b) or Figure 25c), the tail end switch selects the protection trail. If a single point failure cuts both directions of transmission, then both directions of transmission on the working path fail and both directions of transmission switch automatically to the protection trail.

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

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



a) Normal conditions

b) Unidirectional failure (fibre 1)

c) Unidirectional failure (fibre 2)

Figure 25: Two-fibre uniformly routed 1+1 trail protection network with single-ended switching

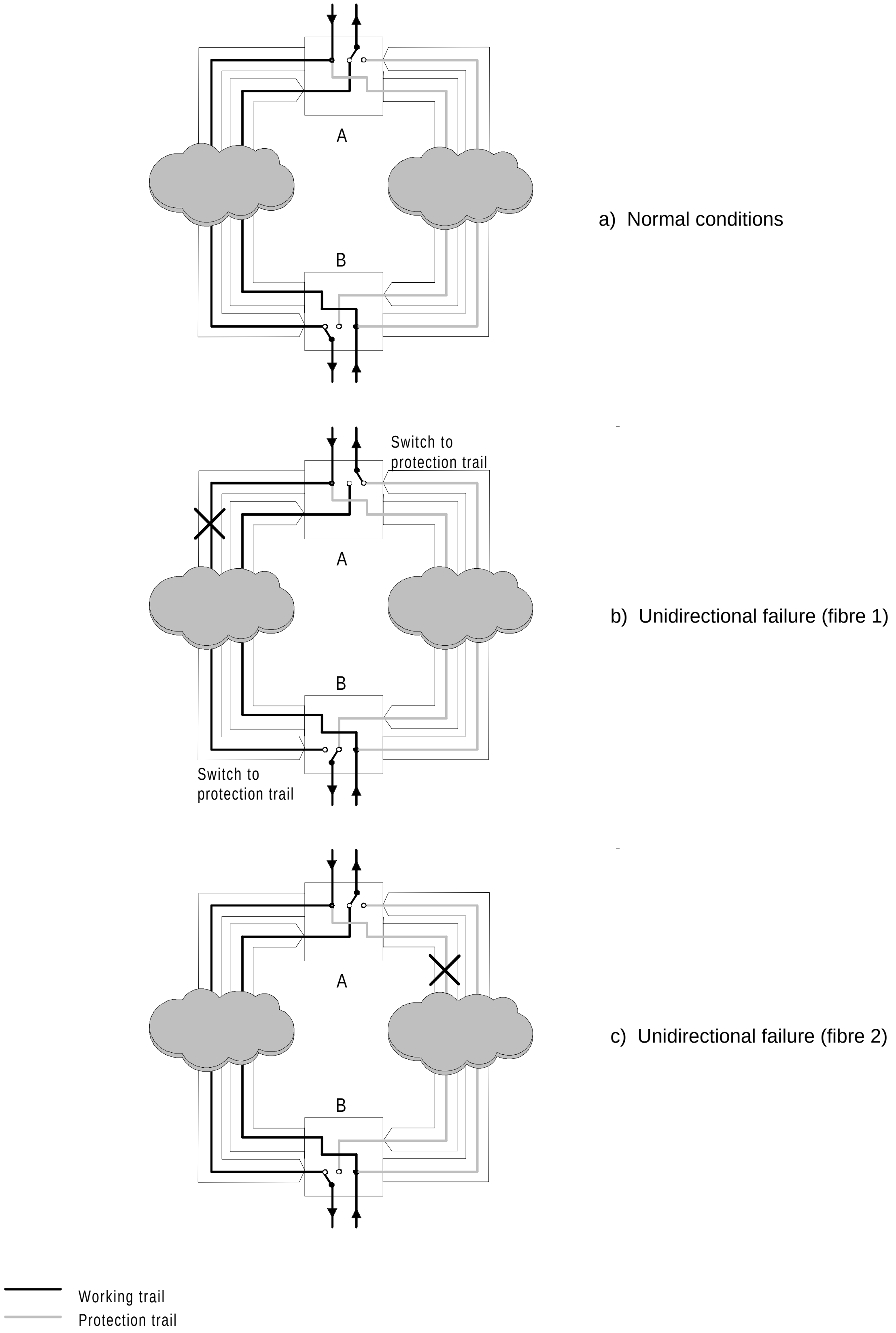
7.3.3 1+1 dual-ended protection

Figure 26a) illustrates a 1+1 diversely routed trail protection network with traffic transmitted between Nodes A and C. Traffic inserted at Node A is transmitted on different trails in two directions to Node C. Under normal operating conditions, the receiver at Node C selects the working traffic. Traffic inserted at Node C is also transmitted in two directions to Node A.

When there is a unidirectional failure on the working trail, as shown in figure 26b), the tail end switch selects the protection trail. For dual-ended switching, an indication is sent via the APS protocol to force the unaffected direction of transmission to also switch to the protection trail. This maintains uniform routeing (i.e. both directions of transmission using the same routes) even under unidirectional failures. If a single point failure cuts both directions of transmission, then both directions of transmission on the working path fail and both directions of transmission switch automatically to the protection trail.

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

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



a) Normal conditions

b) Unidirectional failure (fibre 1)

c) Unidirectional failure (fibre 2)

Figure 26: Two-fibre uniformly routed 1+1 trail protection network with dual-ended switching

7.3.4 1:1 protection

This protection scheme is for further study.

7.3.4.1 Secondary (extra) traffic with 1:1 protection

This protection scheme is for further study.

7.3.5 1:n protection

This protection scheme is for further study.

7.3.5.1 Secondary (extra) traffic with 1:n protection

This protection scheme is for further study.

7.3.6 Traffic misconnection

This is for further study.

7.4 Switch initiation criteria

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

7.5 Functional models

Figure 27 shows the generic 1+1 trail protection functional model. A protection sub layer has been introduced and protection switching is performed by means of the protection Matrix Connection (MCp). In the source direction, the characteristic information from the protected trail is normally permanently bridged onto both outgoing network connections. In the sink direction, the MCp autonomously selects the preferable trail using the Trail Signal Fail (TSF) indications and the information contained in the APS channels. The MCp can be configured via the management system to select the default trail.

Figure 28 shows the generic functional model for 1:1 revertive VC trail protection.

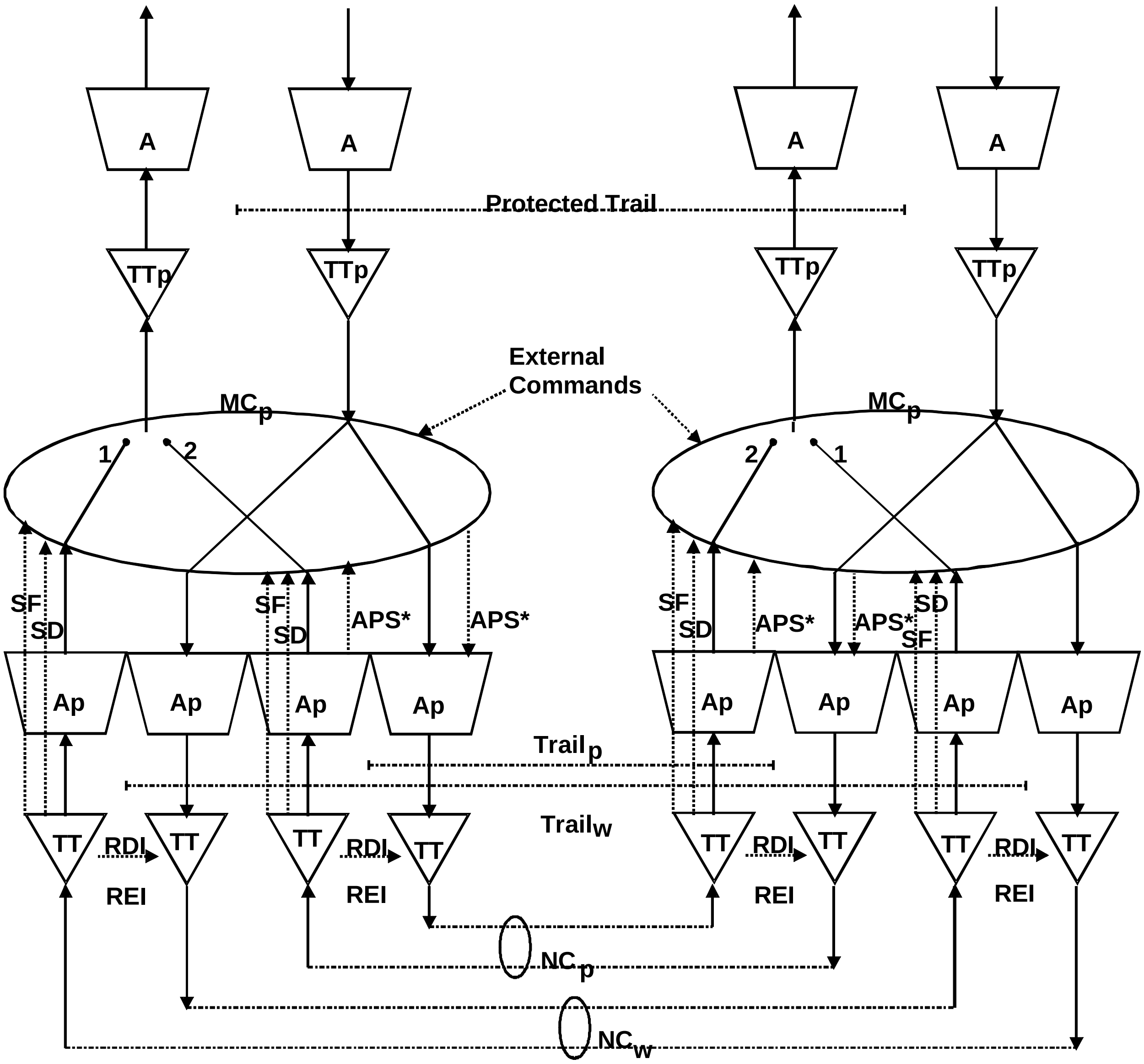
Figure 29 shows the generic functional model for 1:1 non-revertive VC trail protection.

Figure 30 shows a model for a HO VC protection trail indicating the connections in the protection connection matrix when traffic in both directions is carried on the working trails.

Figure 31 shows the functional model for a HO VC protection trail in which there is an interruption in the incoming working trail indicating the corresponding connections in the connection matrix.

Figure 32 shows a model for a LO VC protection trail indicating the connections in the protection connection matrix when traffic in both directions is carried on the working trails.

Figure 33 shows the functional model for a LO VC protection trail in which there is an interruption in the incoming working trail indicating the corresponding connections in the connection matrix.

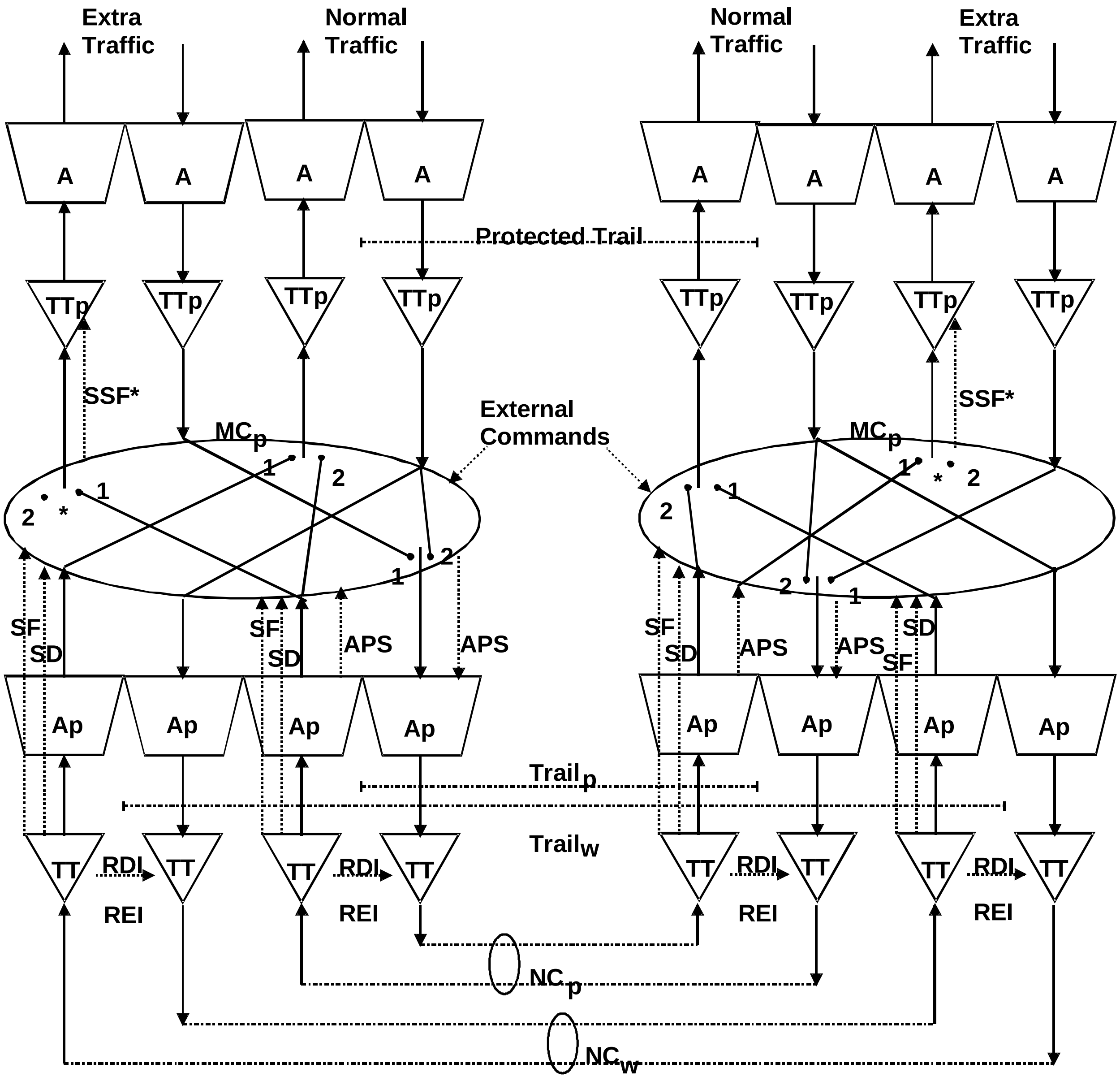


*Required for dual ended switching.
Not required for single ended switching

A	Adaptation	SD	Signal Degrade
Ap	protection Adaptation	SF	Signal Fail
MCp	protection Matrix Connection	SSF	Server Signal Fail
NCp	protection Network Connection	Trailp	protection Trail
NCw	working Network Connection	Trailw	working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TTp	protection Trail Termination

States 1 - Normal state
2 - Failure state

Figure 27: Functional model for generic 1+1 linear trail protection

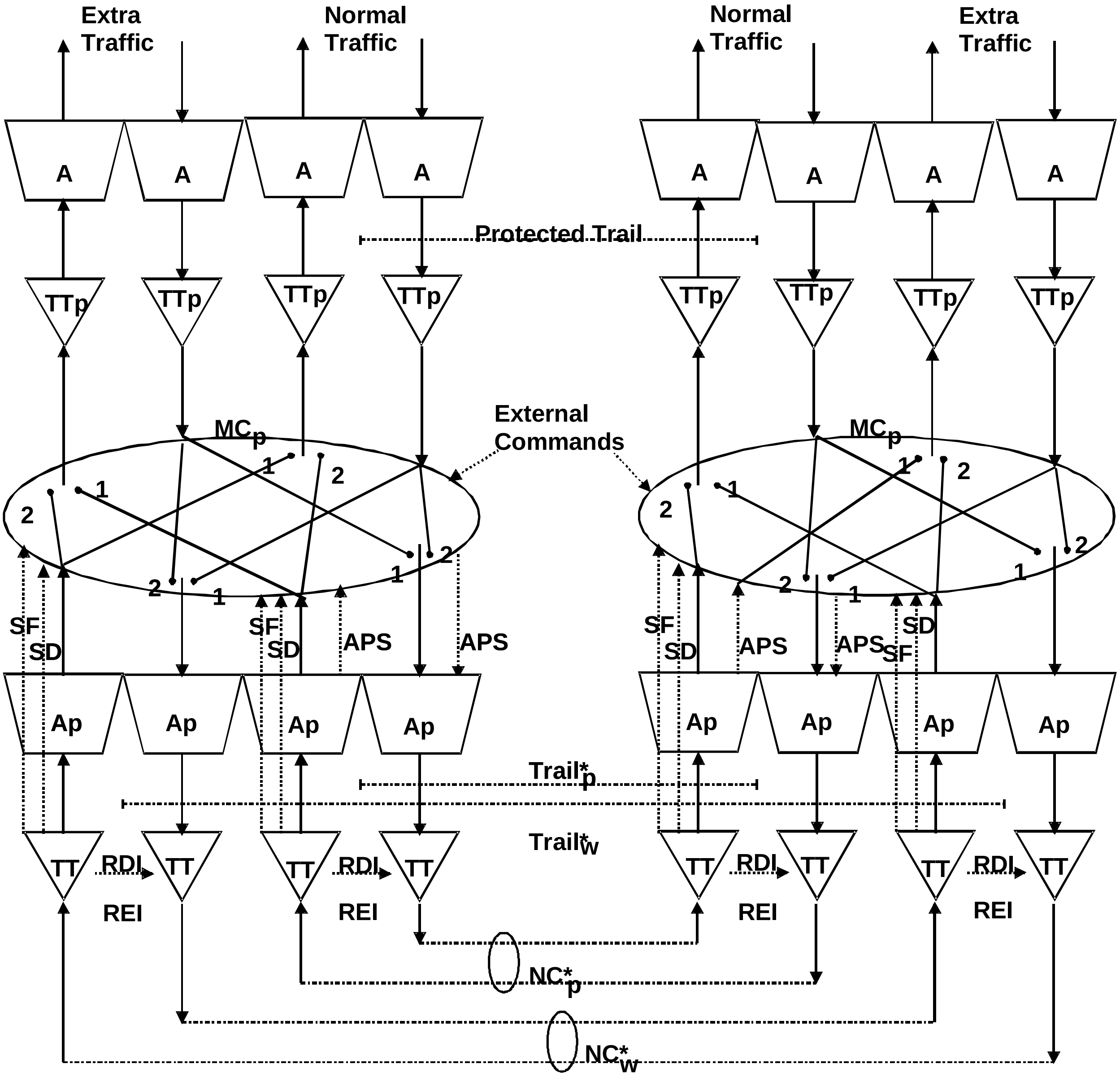


*Required for dual ended switching.
Not required for single ended switching

A	Adaptation	SD	Signal Degrade
Ap	protection Adaptation	SF	Signal Fail
MCp	protection Matrix Connection	SSF	Server Signal Fail
NCp	protection Network Connection	Trailp	protection Trail
NCw	working Network Connection	Trailw	working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TTp	protection Trail Termination

States 1 - Normal state
2 - Failure state

Figure 28: Functional model for generic 1:1 linear trail protection - revertive operation

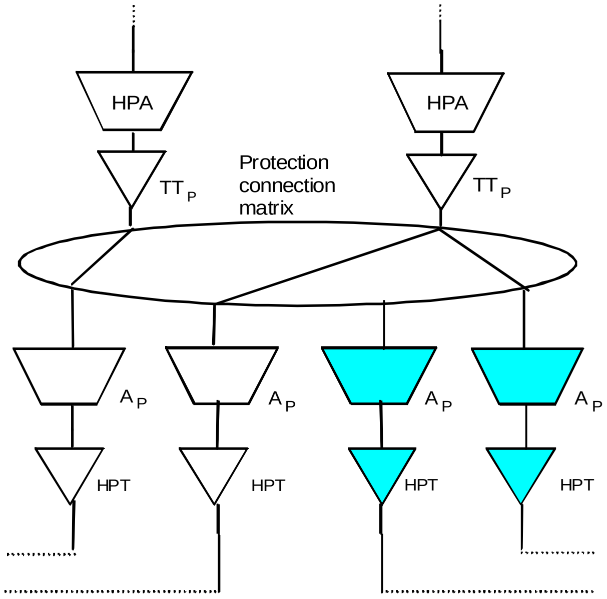


*Required for dual ended switching.
Not required for single ended switching

A	Adaptation	SD	Signal Degrade
Ap	protection Adaptation	SF	Signal Fail
MCp	protection Matrix Connection	SSF	Server Signal Fail
NCp	protection Network Connection	Trailp	protection Trail
NCw	working Network Connection	Trailw	working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TTp	protection Trail Termination

States 1 - Normal state
2 - Failure state

Figure 29: Functional model for generic 1:1 linear trail protection - non revertive operation

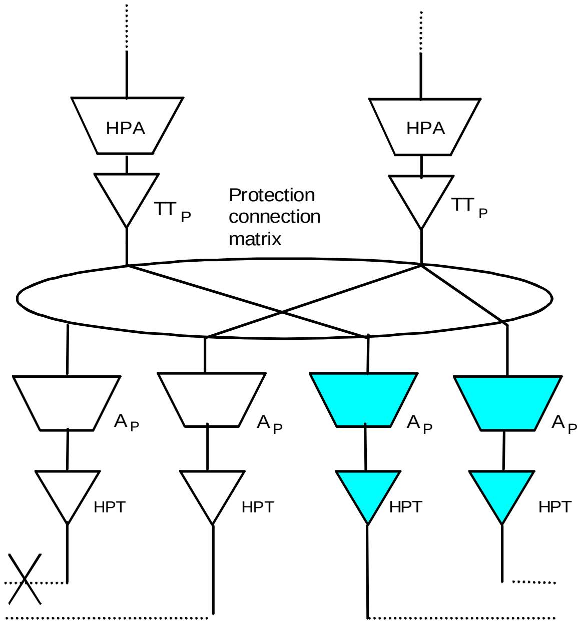


HPT = Higher order Path Termination
HPA = Higher order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 30: Functional model of a HO VC protection trail

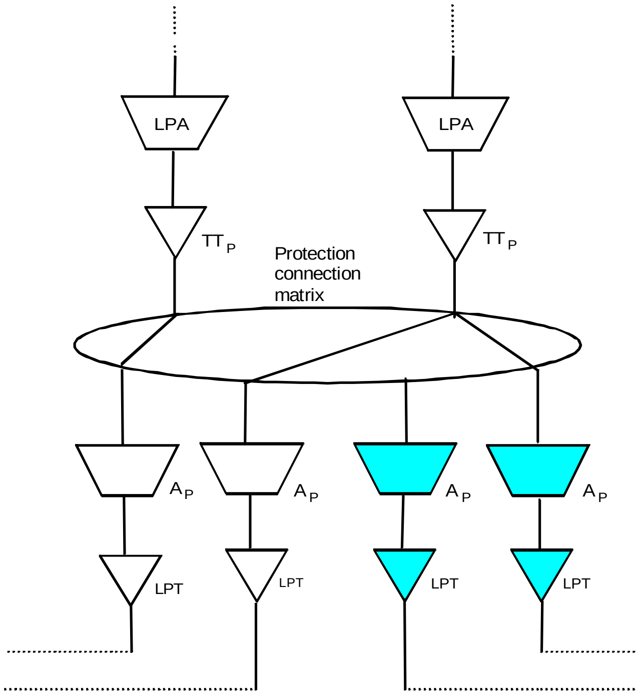


HPT = Higher order Path Termination
HPA = Higher order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 31: Functional model of a HO VC protection trail with a fault on the incoming working trail

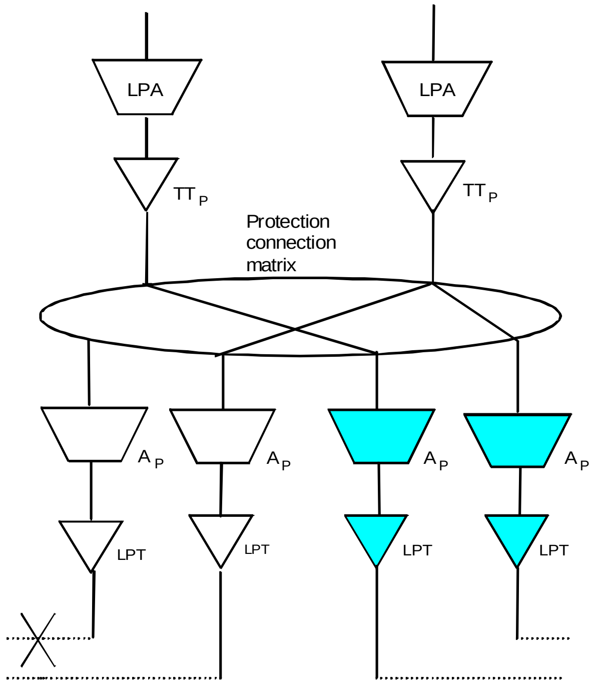


LPT = Lower order Path Termination
LPA = Lower order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 32: Functional model of a LO VC protection trail



LPT = Lower order Path Termination
LPA = Lower order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 33: Functional model of a LO VC protection trail with a fault on the incoming working trail

7.6 Protection interworking

The interworking scenarios between LO/HO trail protection and other schemes are described in TS 101 010 [1].

7.7 APS protocol

Details of the APS protocol and operation for the 1+1 dedicated protection and the dual end protection switching are described in ETS 300 746 [2].

8 SDH Sub-Network Connection (SNC) protection

8.1 Network architecture

Inherently monitored Sub-Network Connection protection (SNC/I) protection, generically, protects against failures in the server layer. The protection process and the defect detection process are performed by two adjacent layers. The server layer performs the defect detection process, and forwards the status to the client layer by means of the server signal fail (SSF) signal.

Non-intrusively monitored Sub-Network Connection protection (SNC/N) protection, generically, protects against failures in the server layer, and failures and degradations in the client layer.

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

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

1:n protection schemes where the protection trail is shared between n working trails is for further study.

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

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

SNC protection does not limit the number of NEs within the SNC/NC.

There are many network configurations where SNC can be used. Figure 34 shows one example of a network consisting of two interconnected two-fibre rings. SNC protection may be required in such a network if, for example, there is an operator boundary between the two rings and individual operators require to be able to protect the sub-network which is within their operating boundary.

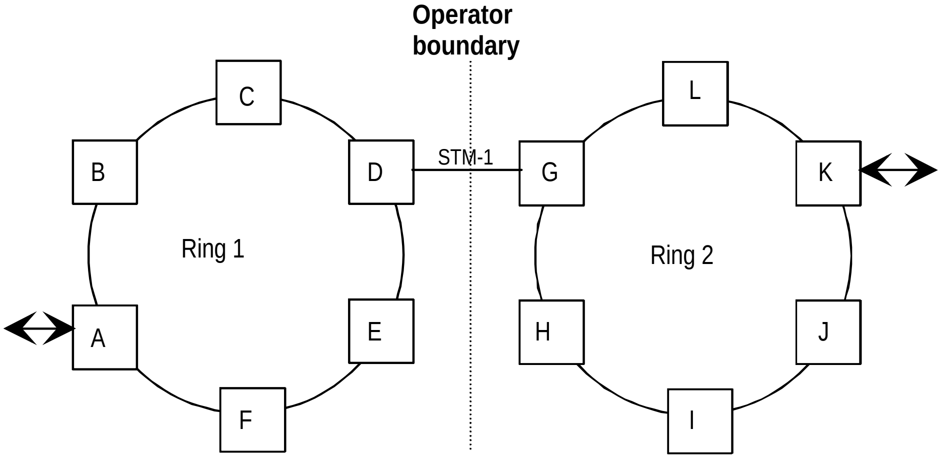


Figure 34 Example of SNC protection in a network with two interconnected rings

NOTE: If a SNC protection is used within a tandem connection sublayer and a failure occurs on the working SNC, the protection switch will not take place due to the presence of the TSF condition on the two SNCs. This will not affect the traffic that is already lost due to a failure outside the tandem connection but causes the TCT sink functions to declare a Tandem Connection fail condition even if the failure could have been restored by the SNCP/N. This situation is described in more detail in annex B.

8.2 Network objectives

The following network objectives apply:

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

2) **Transmission delay:** the transmission delay depends on the physical length and the processing functions within the sub-network. The maximum transmission delay is for further study. Limitations on the transmission delay may be imposed if the target switch completion time for dual-ended operation is to be met;

3) **Hold-off times:** hold-off times are useful for inter-working of protection schemes and these times should be provisionable on an individual VC basis. The failure condition should be continuously monitored for the full duration of the hold-off time before switching occurs. Where digital cross connect equipment is used to carry out the protection switching the switching time may be of the order of seconds. Where a multiplexer equipment is used to implement the switching the switching time will be of the order of 50 ms. The hold-off time should therefore be provisionable from 0 to approximately 20 seconds in steps of the order of 100 ms;

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

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

6) **APS protocol and algorithm:** the SNC protection process should operate in a similar manner at both the HO and LO layers. The minimum requirement is that it can support 1+1 dedicated protection. APS for 1:1 and 1:n protection is for further study;

7) **Operation modes:** non-revertive switching is the minimum requirement for 1+1 protection with single ended switching. Requirements for 1:1 protection are for further study;

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

9) **Switch initiation criteria:** switch initiation should be based on SF and/or SD indications in harmony with definitions used in ITU-T Recommendation G.783 [6];

10) **Upgradability:** it shall be possible to add and delete nodes or upgrade the capacity of a SNC;

11) **Synchronization Distribution:** not applicable.

8.3 Application architecture

8.3.1 Routeing

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

As noted in the network objectives, the network operator has a choice of uniform or diverse routeing on a per-SNC basis. For the simplest case whereby working SNCs and protection SNCs are placed on separate routes, the difference in provisioning a node for uniform routeing versus diverse routeing for 1+1 protection is illustrated in figures 23 and 24. For SNC protection (in contrast to linear VC trail protection), the nodes illustrated may not necessarily terminate the trails involved.

A node using 1+1 uniform routeing under normal operating conditions is shown in figure 23a). A bridge is used to simultaneously transmit signals onto the working and protection SNCs. The receiver uses a switch to select the working SNC under normal operating conditions. Note that the working SNCs are placed on the same facilities (i.e. the left side of the node). Figure 23b) shows the node when there is a failure in the working SNC. In this case, the receiver will detect the loss of signal and will switch to the protection SNC.

A node using diverse 1+1 routeing under normal operating conditions is shown in figure 24a). A bridge is used to simultaneously transmit signals onto the working and protection routes. The receiver uses a switch to select the working SNC under normal operating conditions. Note that the working SNCs are placed on different facilities (i.e. one on the left side of the node, the other on the right). Figure 24b) shows the node when there is a failure in the working SNC. In this case, the receiver will detect the loss of signal and will switch to the protection SNC.

8.3.2 1+1 single-ended protection

Figure 35a) illustrates diversely routed SNC protection with traffic transmitted between nodes A and C. Traffic inserted at Node A is transmitted on different SNCs in separate directions to Node C (e.g. a working SNC and a protection SNC). Under normal operating conditions the receiver at Node C selects the working SNC traffic. When there is a failure on the working SNC, as shown in figure 35b), the tail end switch selects the protection SNC. If there is a failure in the protection SNC, as shown in figure 35c), then the receiver will not need to switch and will continue to detect traffic from the working SNC.

Diversely routed SNCs are capable of surviving certain multiple failures, including cable cuts, if they result in the same SNC being disrupted, as shown in figure 36a). Connectivity will be broken if failures occur which affect both SNCs, as shown in figure 36b). Figure 36c) gives an example of protection switching due to a nodal failure. Traffic terminating at the failed node is disrupted, but traffic passing through to other nodes can survive by switching to the protection SNC.

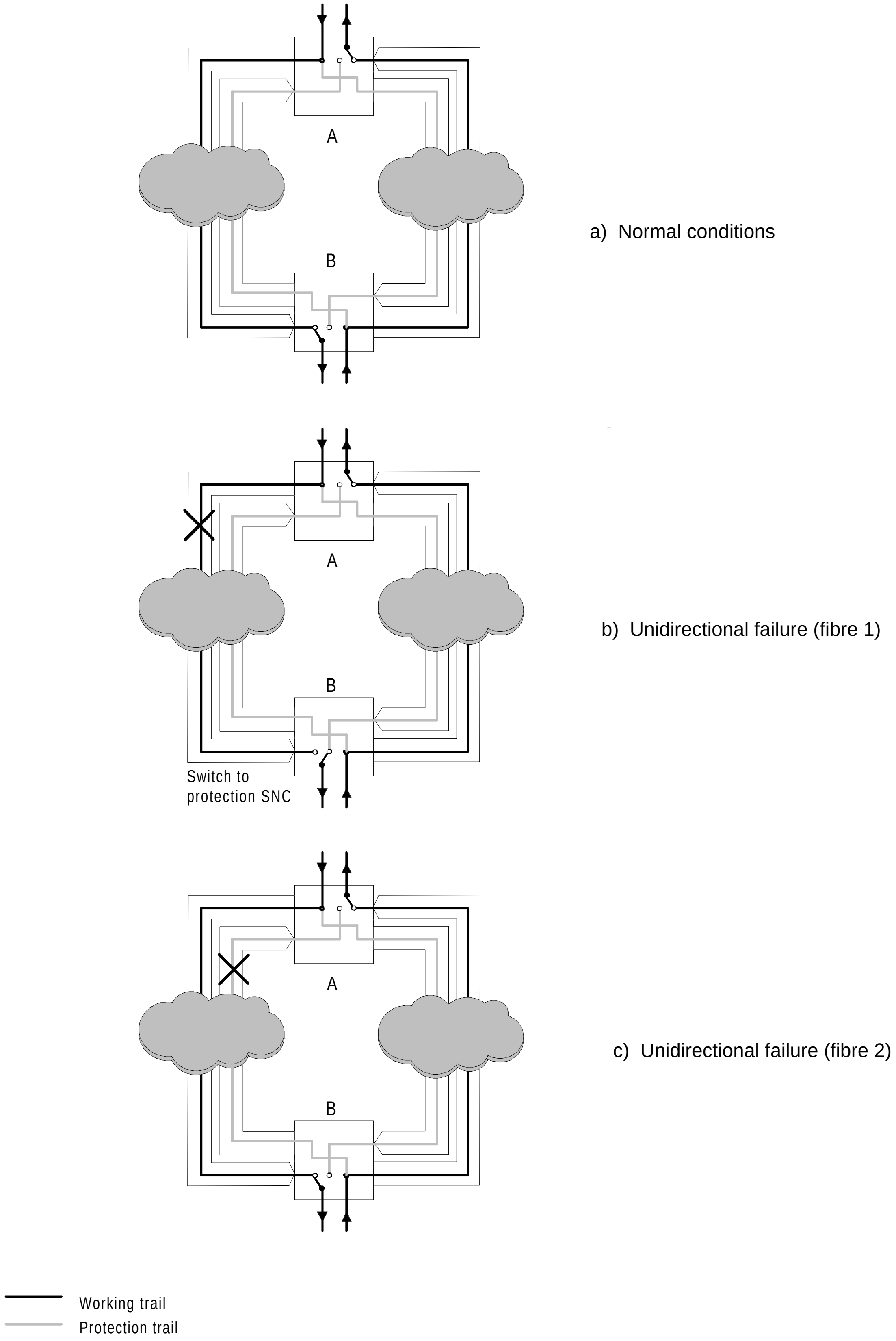
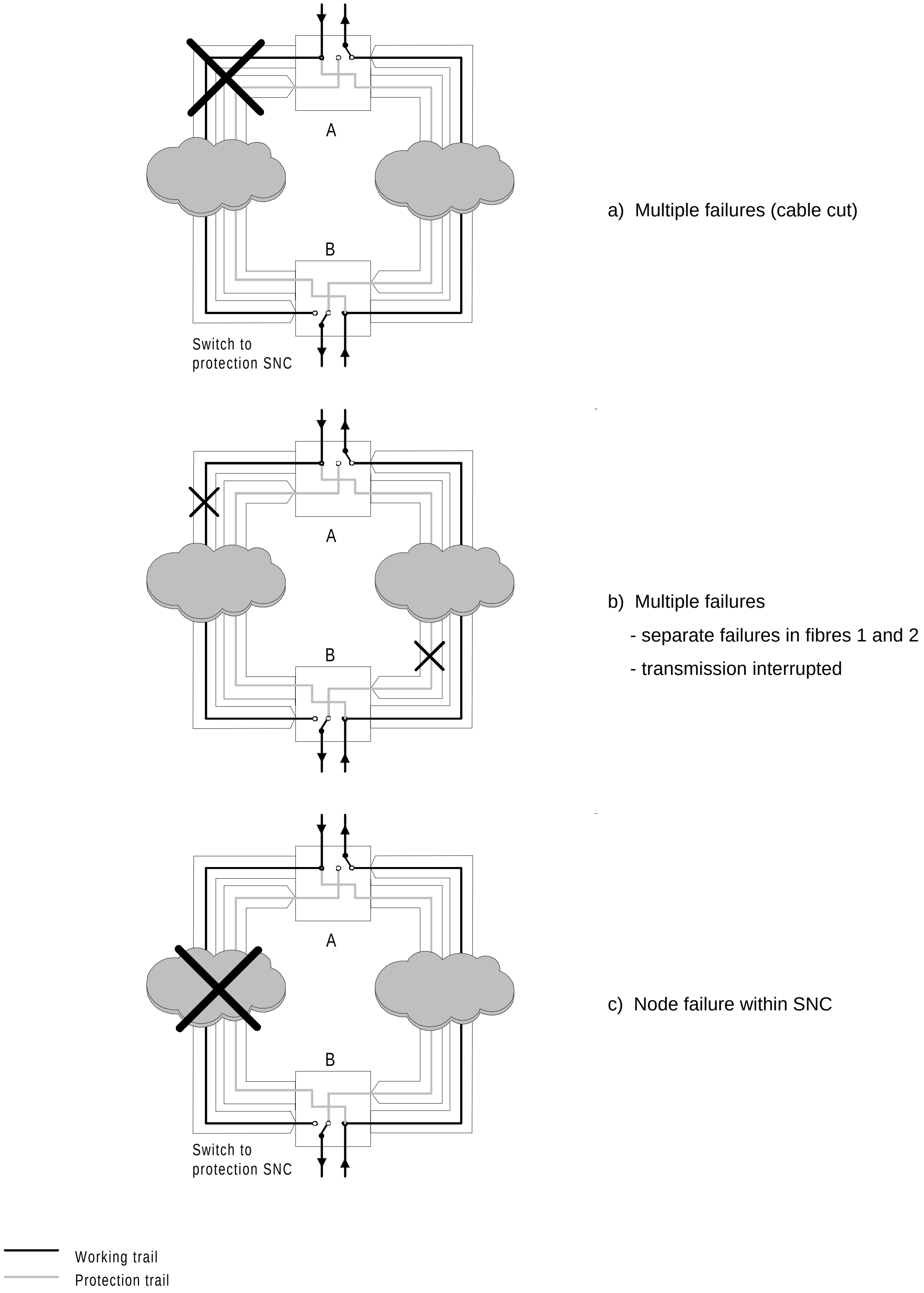


Figure 35: Two-fibre diversely routed 1+1 SNC protection network with a single failure



a) Multiple failures (cable cut)

b) Multiple failures

- separate failures in fibres 1 and 2
- transmission interrupted

c) Node failure within SNC

Figure 36: Two-fibre diversely routed 1+1 SNC protection network with multiple failures

8.3.3 1+1 protection with dual ended switching

This is for further study.

8.3.4 1:1 protection

This is for further study.

8.3.4.1 Secondary (extra) traffic

This is for further study.

8.3.5 1:n protection

This is for further study.

8.3.5.1 Secondary (extra) traffic

This is for further study.

8.3.6 Traffic misconnection

No potential for traffic misconnection exists in 1+1 LO/HO SNC protection networks.

1:1 and 1:n protection schemes are for further study.

8.3.7 Switch initiation criteria

LO/HO SNC 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.

8.3.8 Functional model

Figure 37 shows the generic model for 1+1 SNC protection with inherent monitoring.

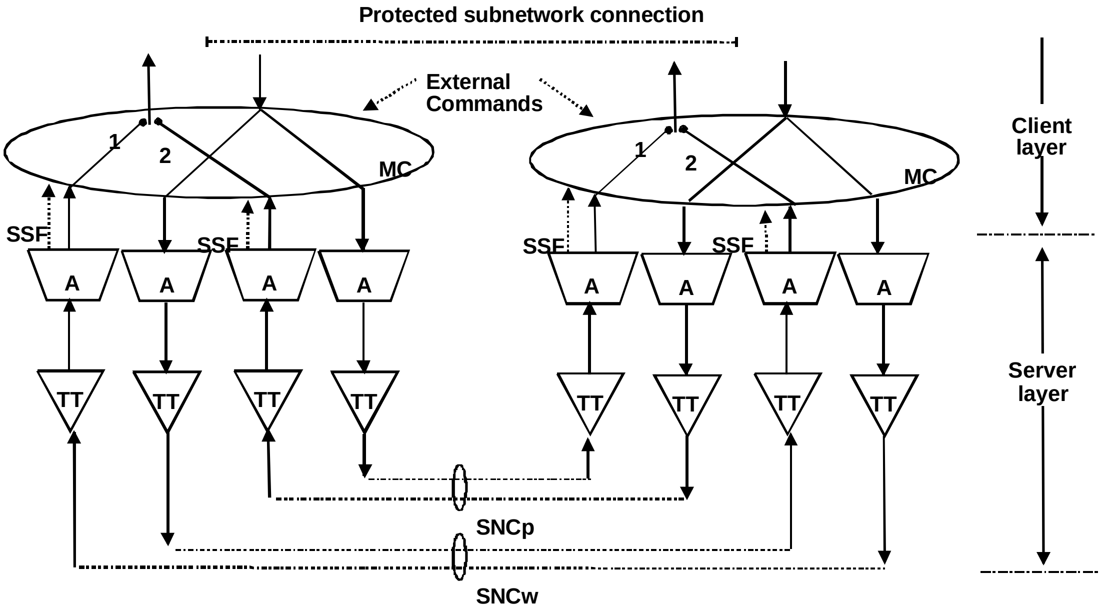
Figure 38 shows the generic model for 1+1 SNC protection with non-intrusive monitoring.

Figure 39 shows a model for a HO 1+1 SNC protection indicating the connections in the protection connection matrix when traffic in both direction is carried on the working SNCs.

Figure 40 shows the functional model for a HO 1+1 working SNC indicating the corresponding connections in the connection matrix.

Figure 41 shows a model for a LO 1+1 SNC protection indicating the connections in the protection connection matrix when traffic in both direction is carried on the working SNC.

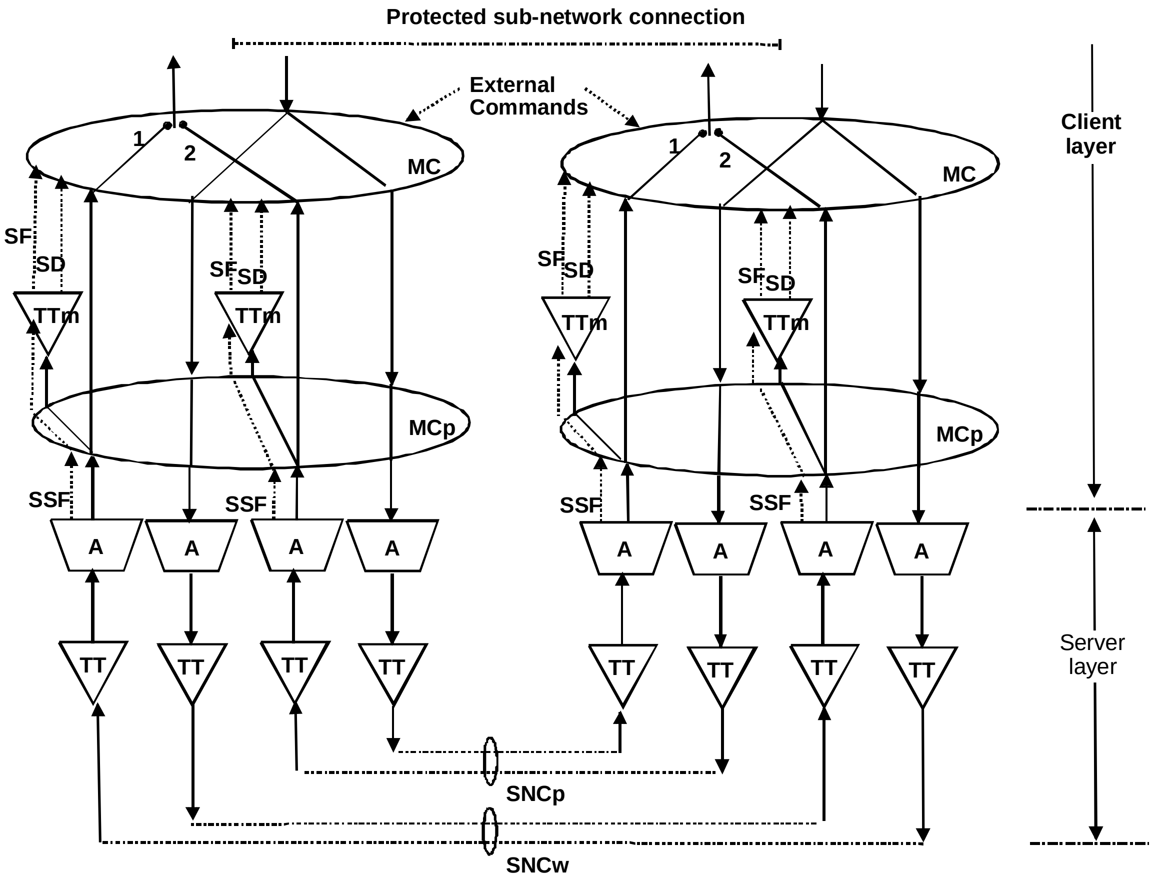
Figure 42 shows the functional model for a LO 1+1 SNC protection in which there is an interruption in the incoming working SNC indicating the corresponding connections in the connection matrix.



A = Adaptation
MC = Matrix Connection
SNCp= protection Sub-Network Connection
SNCw= working Sub-Network Connection
SSF = Server Signal Fail
TT = Trail Termination

States:
1 - Normal state
2 - Failure state

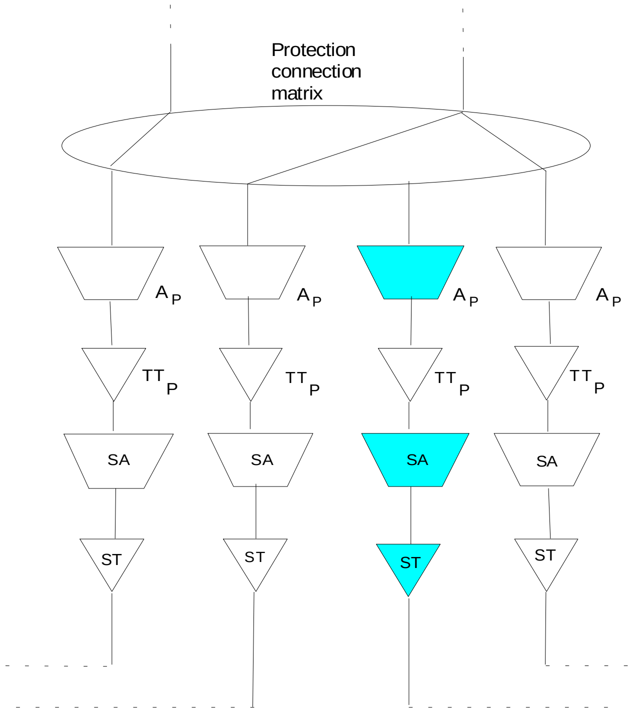
Figure 37: Functional model for SNC protection with Inherent monitoring (SNC/I) by means of a server signal fail



A = Adaptation
MC = Matrix Connection
MCp = protection Matrix Connection
SD = Signal Degrade
SF = Signal Fail
SNCp= protection Sub-Network Connection
SNCw= working Sub-Network Connection
SSF = Server Signal Fail
TT = Trail Termination
TTm = non-intrusive monitor

States:
1 - Normal state
2 - Failure state

Figure 38: Functional model for SNC protection with non-intrusive monitoring (SNC/N)

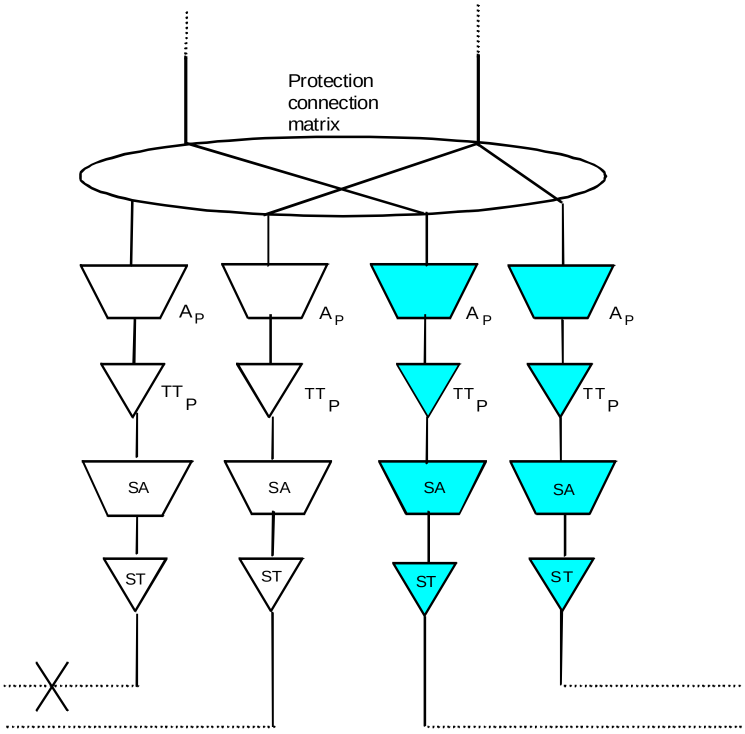


ST = Section Termination
SA = Section Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 39: Functional model for HO SNC protection

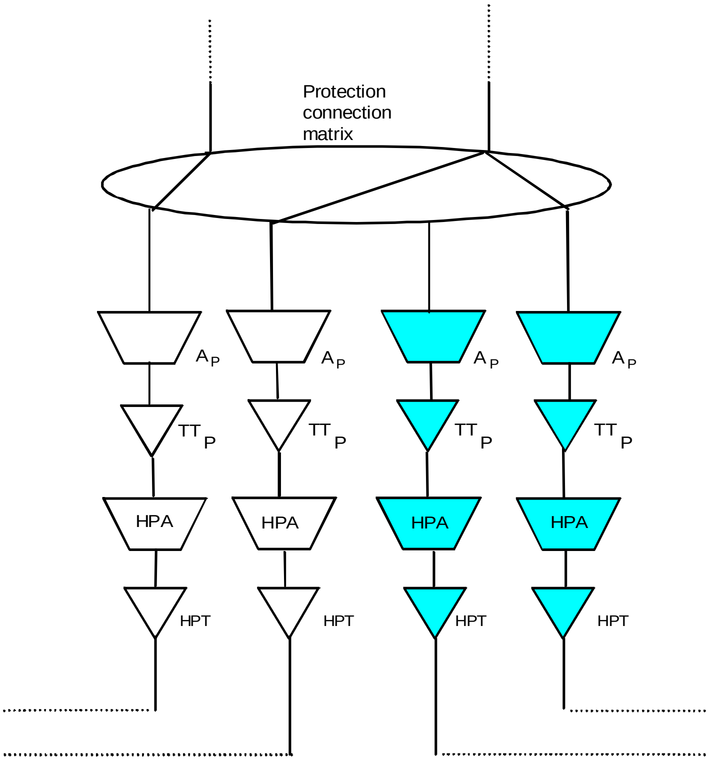


ST = Section Termination
SA = Section Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 40: Functional model for HO SNC protection with a fault on the incoming working SNC



HPT = Higher order Path Termination
HPA = Higher order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation

□ Working

🟦 Protection

Figure 41: Functional model for LO SNC protection

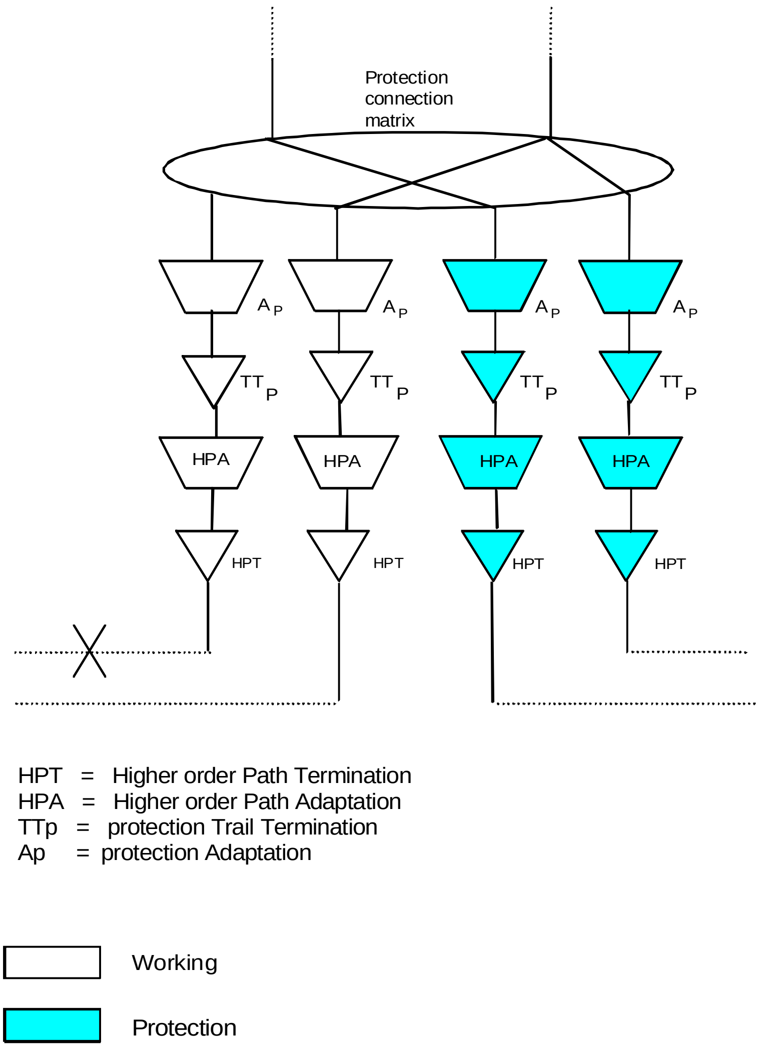

Protection
connection
matrix
A P
TT P
HPA
HPT
HPT = Higher order Path Termination
HPA = Higher order Path Adaptation
TTp = protection Trail Termination
Ap = protection Adaptation
Working
Protection

Figure 42: Functional model for LO SNC protection with a fault on the incoming working SNC

8.3.9 Protection interworking

The interworking scenarios between LO/HO SNC protection and other schemes are described in TS 101 010 [1].

8.3.10 APS protocol

A protocol will be required if dual ended switching is used.

Details of the APS protocol are described in ETS 300 746 [2].

9 Comparison of protection schemes

Table 1 makes a comparison of SDH protection schemes for a range of functions. The relative advantage of each scheme for each function is indicated by the number of crosses.

NOTE 1: The comparison is made on a per function basis (e.g. row by row) and it is not appropriate to compare rows.

NOTE 2: The size, complexity and cost of each scheme has not been taken into account in making this comparison table.

Table 3: Comparison of SDH protection schemes

	MS Linear	**MS SPRing**	**MS DPRing**	**HO VC Trail**	**LO VC Trail**	**HO SNC/I (note 3)**	**HO SNC/N (note 3)**	**LO SNC/I (note 3)**	**LO SNC/N (note 3)**
Bandwidth efficiency (note 2)	**X**	**XX**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Ability to protect a selected part of the traffic	**No**	**(note 4)**	**(note 5)**	**X**	**XX**	**X**	**XX**	**XX**	**XX**
Compatibility with secondary traffic	**X**	**XX**	**X**	**XX**	**XX**	**X**	**X**	**X**	**X**
Level of protection		**X**	**X**	**XX**	**XXX**	**XX (note 1)**	**XX (note 1)**	**XXX (note 1)**	**XXX (note 1)**
Response time	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Transmission delay	**XXX**	**XX**	**X**	**XXX**	**XXX**	**XXX**	**XXX**	**XXX**	**XXX**
Multiple failures in a cascade of sub-networks	**XX**	**XXX**	**XXX**	**X**	**X**	**XX**	**XX**	**XX**	**XX**
Interworking	See TS 101 010 [1] for information on protection interworking.								
Applicable to network architectures other than rings	**X**			**X**	**X**	**X**	**X**	**X**	**X**
Connection type: Sub-network (S) End to end (E)	**S**	**S**	**S**	**E**	**E**	**SE**	**SE**	**SE**	**SE**

NOTE 1: SNC/I and SNC/N have different levels of protection (see subclause 9.11).
NOTE 2: Only applicable to ring topologies.
NOTE 3: See comparison of SNC/I and SNC/N in subclause 9.11.
NOTE 4: Enhancements of the MS SPRing to allow selected protection of HO VCs has not been fully described and therefore a comparison cannot be made. This is for further study.
NOTE 5: Enhancements of the MS DPRing to allow selected protection of HO/LO VCs has not been fully described and therefore a comparison cannot be made. This is for further study.

9.1 Bandwidth efficiency

Figure 43 shows the ratio of the required capacity for a MS DPRing and a MS SPRing based on the calculations presented in annex A. This is for a traffic demand of one VC-4 between any two nodes and for three different traffic patterns. (uniform, double hub and site to adjacent site).

It can be seen from Figure 43 that the MS SPRing requires less capacity than the MS DPRing to support one VC-4 traffic demand between any two nodes in the case of uniform or adjacent traffic patterns. Due to the shared protection mechanism the VC-4 bandwidth efficiency for MS SPRing can be very high for site to adjacent site traffic.

For the uniform and adjacent traffic pattern the maximum number of nodes supported by the MS SPRing is also substantially larger.

For uniform traffic, the maximum number of nodes for a STM-16 MS DPRing is six. 15 VC-4s are required for this number of nodes (see subclause A.5). For a STM-16 MS SPRing the maximum number of nodes is seven and this requires 12 VC-4s (see subclause A.5).

In the case of the double hub traffic pattern the maximum number of nodes for both STM-16 MS DPRing and MS SPRing is 10 and all 16 VC-4s are used with 10 nodes (see subclause A.5).

NOTE 1: This assumes the worst case scenario in which the hub nodes are adjacent.

In the case of a site to adjacent site traffic pattern, the STM-16 MS DPRing can not support more than 16 nodes due to capacity limitations; with 16 nodes all 16 VC-4s are used. In the case of a STM-16 MS SPRing only two VC-4s are needed, but the protocol does not support more than 16 nodes.

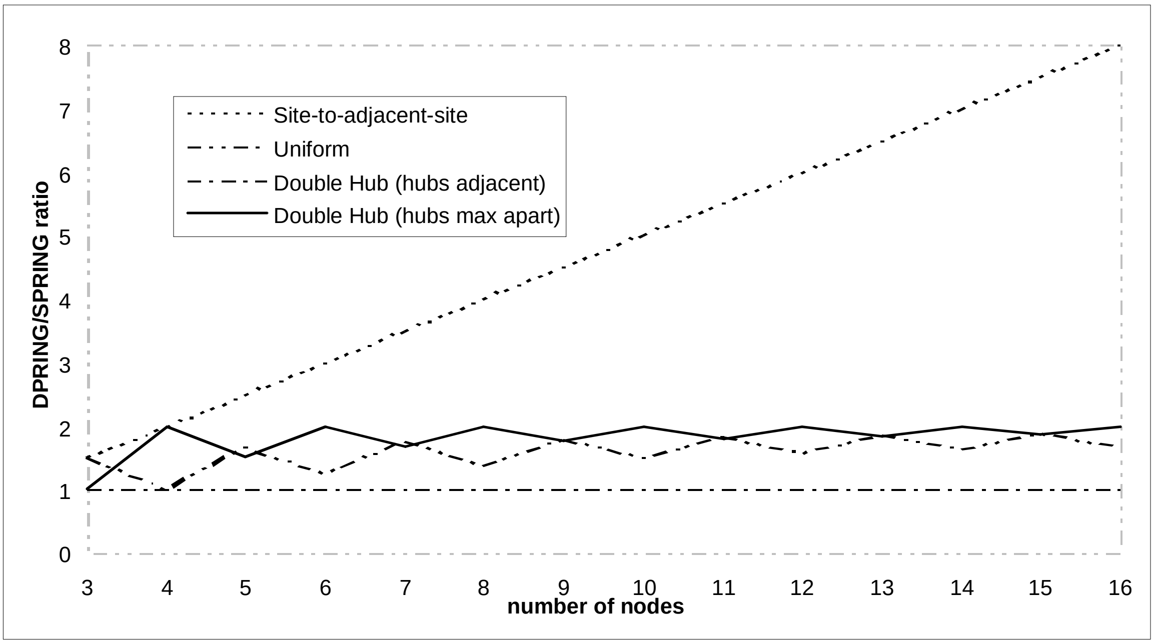


Figure 43: Ratio of required capacity between the MS DPRing and the MS MSPRing for one VC-4 traffic demand

In figure 44 the ratio of the maximum amount of traffic that can be carried on a STM-16 MS SPRing and MS DPRing with VC-4 granularity as a function of the number of nodes in the ring is shown for three different traffic patterns:

- site to adjacent site;
- double hub (where the hub nodes are adjacent);
- uniform.

For example, in the case of nine nodes and a site-to-adjacent-site traffic pattern, the MS SPRing can carry eight VC-4s, while the MS DPRing can carry one VC-4, which gives a maximum capacity ratio of eight.

NOTE 2: The curve shown for the double hub where the hub nodes are adjacent is the worst case condition; the MS SPRing has a substantial advantage over the MS DPRing in the case of a double hub traffic pattern where the two hubs are not adjacent.

The line for a particular traffic pattern ends when the MS DPRing or the MS SPRing is not able to support more nodes. e.g. the line for the uniform traffic pattern ends at six nodes, which is the maximum for the MS DPRing, while the MS SPRing can support seven nodes (see annex A).

For the adjacent traffic pattern the maximum number of nodes is sixteen in both cases, for the MS DPRing due to the maximum capacity, for the MS SPRing due to the protocol limitations. For the double hub with adjacent nodes traffic pattern, the maximum is ten nodes for both schemes. For the double hub traffic pattern with "opposite" nodes, the maximum number of nodes is ten for the MS DPRing and sixteen for the MS SPRing (limited by the protocol) (see annex A).

It should be noted that the capacity comparison of this paragraph deals with specific traffic patterns in which the traffic demands between the nodes are known in advance. When trying to apply the comparison to actual traffic demands which may imply a mix of the above patterns, the exact inter-node traffic may not be known in advance. This may decrease the bandwidth utilization of the MS SPRing, but not that of dedicated protection schemes. This decrease could be avoided by applying timeslot interchange (although this is not currently supported for MS SPRing) or by traffic re-arrangement which may cause traffic interruptions.

NOTE 3: MS DPRing, 1+1 SNCP and 1+1 VC trail protection are essentially equivalent in terms of capacity utilization when applied to the same topology.

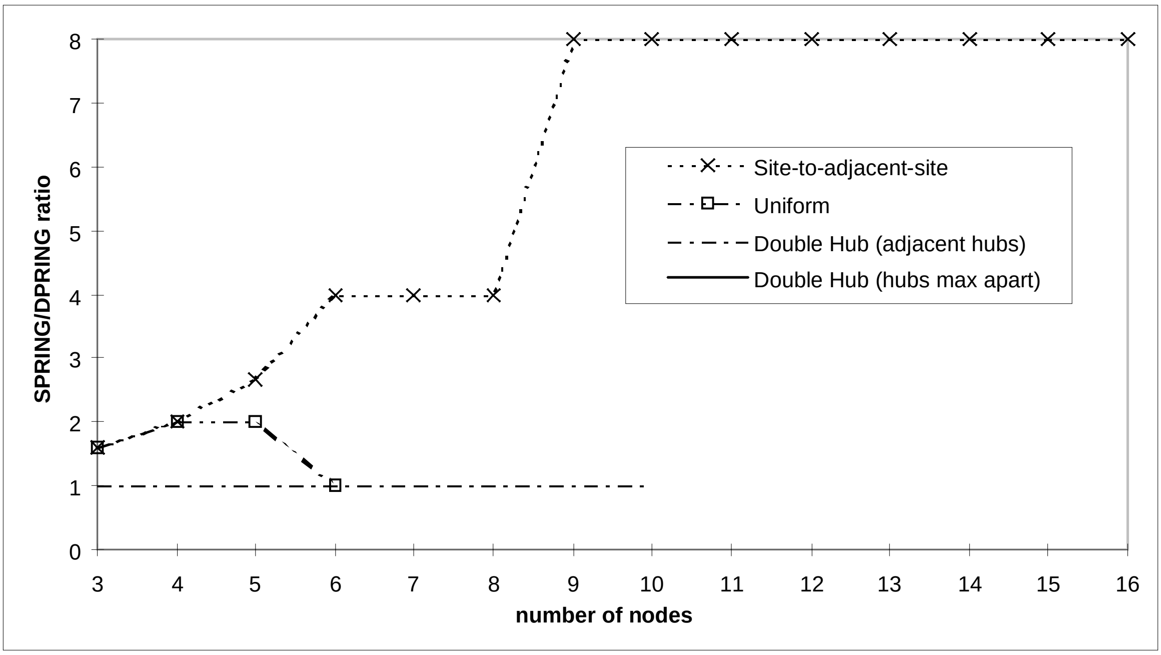


Figure 44: Maximum VC-4 capacity ratio (MS SPRing/MS DPRing) for a STM-16 ring with VC-4 granularity

9.2 Capability to protect a selected part of the traffic

This indicates whether it is possible to have some protected VCs and some unprotected VCs.

MS DPRing, LO VC trail protection and LO SNC protection allow the possibility of exchanging part of the protected traffic for unprotected traffic for HO and LO VCs.

For HO VC trail protection and HO SNC protection, the same is true but only for HO VCs.

MS SPRing does not allow for exchanging protected traffic for unprotected traffic. (An enhanced version may allow this, but this has currently not been fully described - see subclause 6.2.11).

9.3 Compatibility with secondary traffic

This indicates the ability to be able to use the protection capacity for secondary traffic when it is not being used for protection.

SNCP with secondary traffic is not possible because of interworking problems in the case of drop and continue and dual ended switching.

Additional traffic requires a protocol in the case of MS DPRing.

MS SPRings and HO/LO VC trail protection can support secondary traffic.

NOTE: For HO/LO trail protection the secondary traffic would only allow secondary traffic for the same customer.

9.4 Level of protection

This considers the level of protection provided by each scheme e.g.:

- MS schemes protect against Section level failures;
- HO SNC and HO VC trail schemes protect against Section and HO VC failures;
- LO SNC and LO VC trail schemes protect against Section, HO VC and LO VC failures.

9.5 Response time

All mechanisms have the same target response time. 50 ms is the requirement for MS SPRing and MSDPRing schemes given the conditions specified for operation.

There is some concern about the target response when a large number of VCs or SNCs are switched.

Interworking between several protection mechanisms can lead to the use of hold off times.

The comparison does not take into account of the case of secondary traffic in MS SPRings.

9.6 Transmission delay

This relates to the difference between normal operation and operation under failure conditions.

MS DPRing gives the worst case transmission delay because of the uniform routeing characteristic.

MS DPRing and MS SPRing can both give rise to a large transmission delay under failure conditions. The additional delay is dependent on the size of the ring.

9.7 Multiple failures in a cascade of sub-networks

This comparison assumes the interconnection of sub-networks using the same protection scheme.

VC trail protection can generally only cope with a single failure.

SNC and MS SPRing protection can protect against several multiple failure scenarios.

MS SPRing and MS DPRing can additionally withstand a failure of an interconnecting node together with a link failure as shown in figure 45.

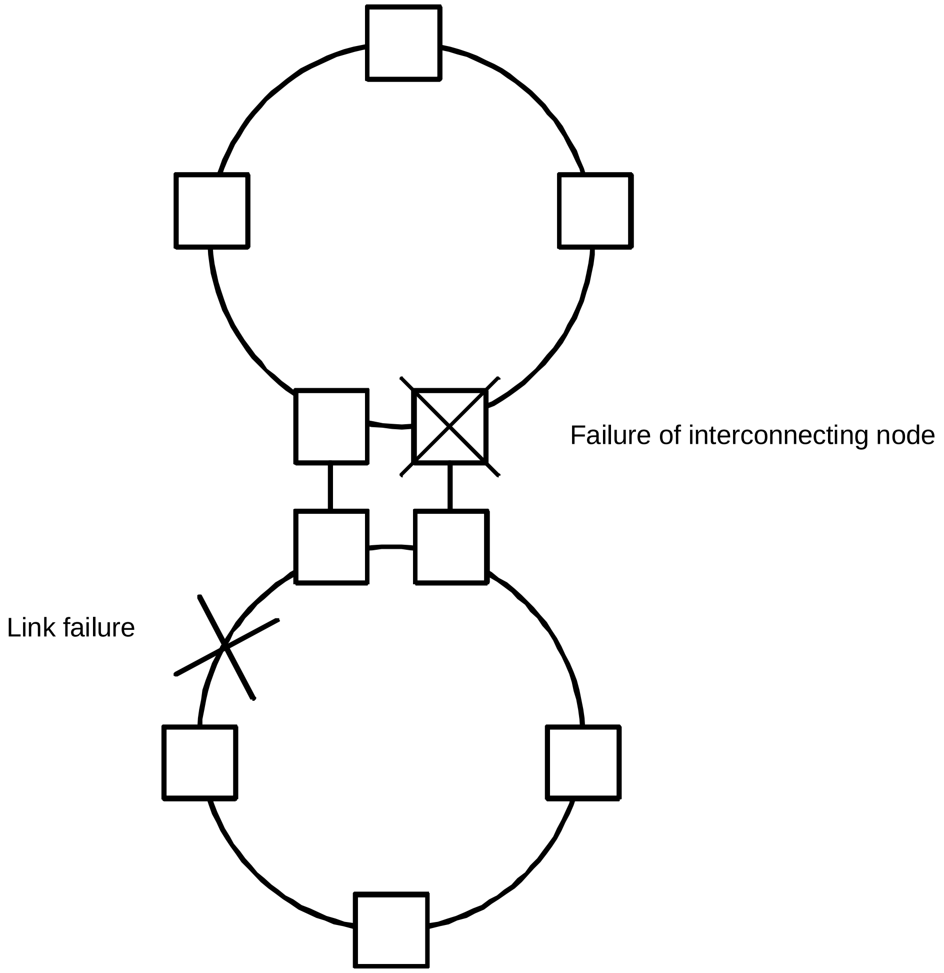


Figure 45: Example of a double failure scenario that can be survived when MS SPRing or MS DPRing protection schemes are used in each ring

9.8 Interworking

This is considered in detail in TS 101 010 [1].

9.9 Applicable to network architectures other than rings

MS SPRing and MS DPRing schemes can only be applied to ring architectures.

SNC and VC Trail protection schemes can be applied to rings or other network architectures.

9.10 Connection type

The protection schemes are compared based on:

- protection per sub-network;
- end to end protection (trail termination to trail termination).

MS SPRing and MS DPRing schemes are for sub-networks, e.g. assuming the path terminations are outside the ring.

VC trail protection is for end to end protection only.

SNCP provides the capability for supporting end to end protection and per sub-network protection.

9.11 A comparison of SNC/I and SNC/N

As stated in subclause 8.1, SNC/I, protects against signal failures in the server layer. Whereas by the use of non intrusive monitoring SNC/N is additionally able to protect against signal failures and signal degrade in the client layer.

Protection switching using HO SNC/I is based on (see ETS 300 746 [2]):

- Higher order Path - Server Signal Fail (HP-SSF) (This includes AU - Loss of Pointer (AU-LOP) and AU-AIS).

Protection switching using HO SNC/N is based on (see ETS 300 746 [2]):

- High order Path - Server Signal Fail (HP-SSF) (This includes AU Loss of Pointer (AU-LOP) and AU-AIS);
- HO Path UNEQuipped defect (HP-UNEQ);
- HO Path Trace Identifier Mismatch (HP-TIM);
- HO Path EXCessive error (HP-EXC);
- HO Path signal Degrade (HP-Degrade).

Protection switching using LO SNC/I is based on (see ETS 300 746 [2]):

- Lower order Path - Server Signal Fail (LP-SSF) (This includes TU Loss of Pointer (TU-LOP) and TU-AIS).

Protection switching using LO SNC/N is based on (see ETS 300 746 [2]):

- Lower order Path - Server Signal Fail (LP-SSF) (This includes TU Loss of Pointer (TU-LOP) and TU-AIS);
- LO Path UNEQuipped defect (LP-UNEQ);
- LO Path Trace Identifier Mismatch (LP-TIM);
- LO Path EXCessive error (LP-EXC);
- LO Path signal Degrade (LP-Degrade).

NOTE 1: SNC/I is simpler and therefore requires less circuitry to implement.

NOTE 2: SNC/N provides a more comprehensive protection capability. Because SNC/N is able to protect against signal failures and signal degrade in the client layer it provides a similar protection capability to VC trail protection.

NOTE 3: The switching criteria for SNC/I does not include trace identifier mismatch and unequipped. In the network scenario shown in figure 46, the condition could therefore arise in which a signal is mis-routed over the sub-network between nodes A and B, the mis-routeing is not detected at the SNC/I protection switch and therefore the signal gets incorrectly transmitted on to the following sub-network. At the trail termination (C) the incorrect signal will be detected and AIS will be inserted as shown in figure 46.

If SNC/N is used, then the trace mismatch at B will be detected and the SNCP will switch to the protection trail as shown in figure 47. The correct signal will then be transmitted to C and so AIS will not be inserted.

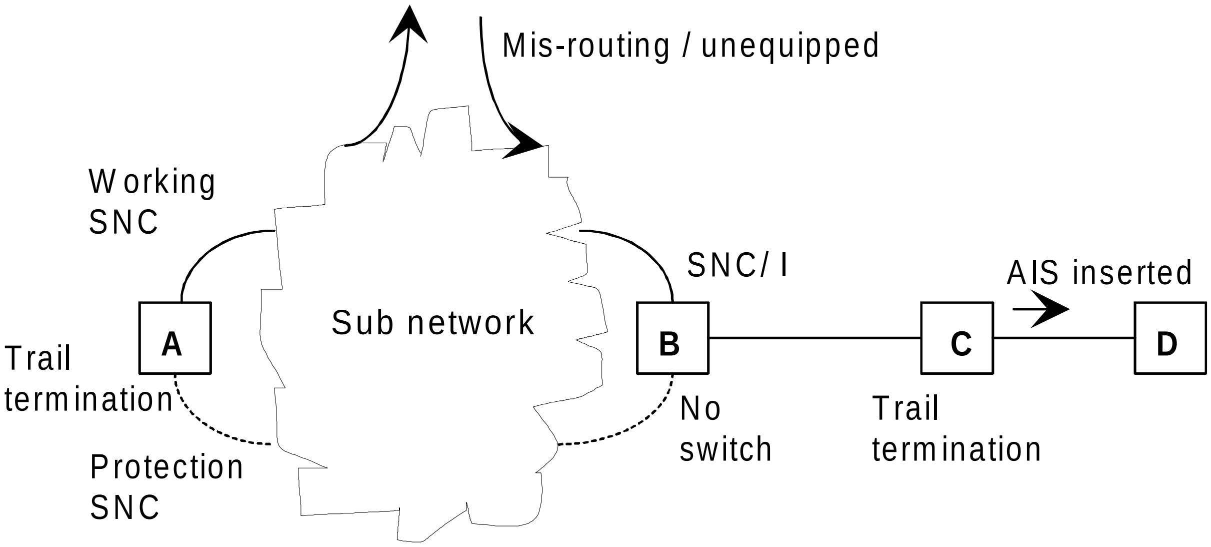


Figure 46: Network example using SNC/I

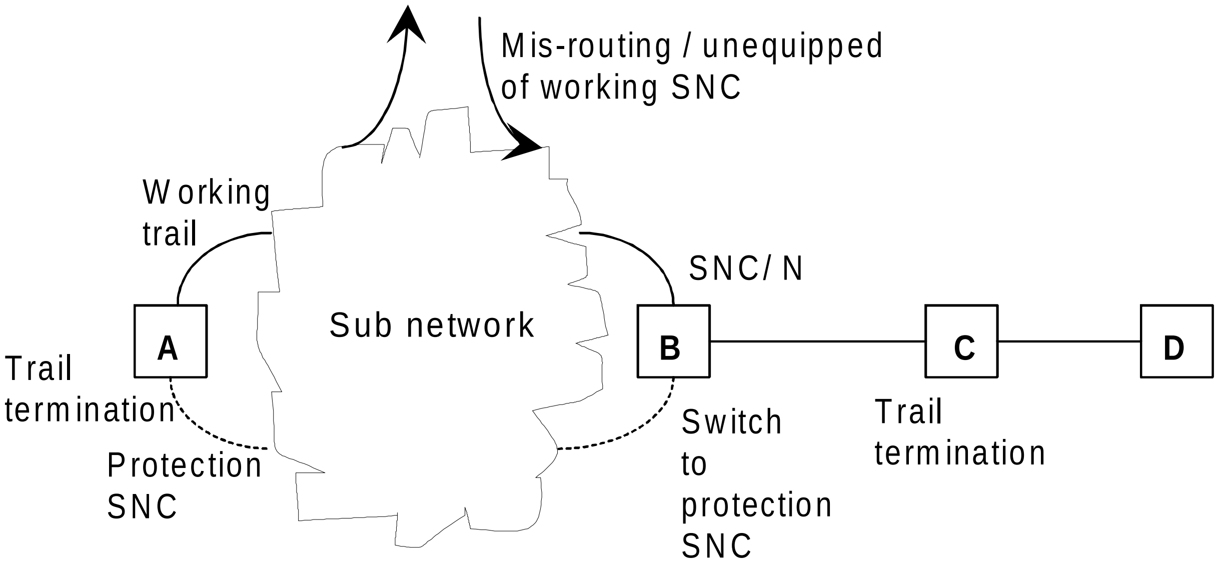


Figure 47: Network example using SNC/N

9.12 LO VC access in a MS SPRing

This is for further study.

10 Examples of network protection applications

10.1 General objectives of protection

General protection objectives are given in subclause 5.4.

10.2 Core network

10.2.1 Core network characteristics

The SDH core transport network has the following characteristics:

- high speeds are predominant, STM-16 and higher in the future;
- traffic patterns are frequently uniform;
- routeing functionality predominantly at the VC4 level.

Another important aspect is the characteristic of the traffic. The basic transport entity in the core network is the VC-4 (in the future it could be also the VC-4-Nc for the introduction of broadband services). Each VC-4 is generally the result of the grooming of different services: voice, data, video, and ATM, for instance. If the traffic is groomed, the option exists to protect all traffic or only that portion of it which requires protection. The option to apply selective protection will be applicable when there is sufficient traffic of both requirements to allow grooming into protected and unprotected VC4s whilst maintaining a good level of fill across the network.

The VC-4s, transported over the core network, may be generated outside of the core network. Therefore the need arises to protect a VC-4 without having the VC trail termination within the core network.

10.2.2 Protection schemes applied to the core network

10.2.2.1 MS-SPRing

A typical architecture for the core network is a meshed network composed by HO-DXC. As the DXC available up to now are generally equipped only with STM-1 interfaces, STM-16 line systems are required for their interconnection; this network architecture is shown in figure 48.

Assuming that the amount of traffic in the network does not allow the grooming into protected and unprotected VCs, selective protection is not possible and the whole traffic has to be protected. In this case, an MS trail protection scheme could be a good solution because protects against the most common fault causes and offers a fast protection switching.

Among the different MS trail protection schemes available, the MS-SPRing offers advantages in term of bandwidth utilization due to the traffic distribution in the core network.

The application of MS-SPRing is perfectly compatible with the present long distance network architecture with HO-DXC and terminal multiplexers. Covering the network with rings has no impact on the network physical topology and the present point-to-point line systems can be converted in MS-SPRings by upgrading the Terminal Multiplexers to Add Drop Multiplexers, as shown in figure 49.

Of course some protection capacity has to be introduced, requiring an increase of the total transmission capacity of the network, but no changes are required in the number of ports and matrix dimension of DXC from the unprotected network to the network protected with MS-SPRings.

The HO-DXCs allow flexible interconnection of the rings. Two options are possible: single homing and dual homing, the second one allowing protection against HO-DXC failures (see TS 101 010 [1]).

If the protection against the failure of the interconnection point between two rings is required, but the frequency of this kind of failure is low enough to allow a slower reconfiguration, a different solution can also be adopted. The rings can be interconnected using single homing and a restoration mechanism at VC-4 level performed by the HO-DXC can be introduced as a second level of protection against the failures not protected by the MS-SPRings.

In some cases the regional network has characteristics of traffic distribution which are similar to the one in the core network. In these cases the same protection scheme used in the core network are also applicable to the regional network.

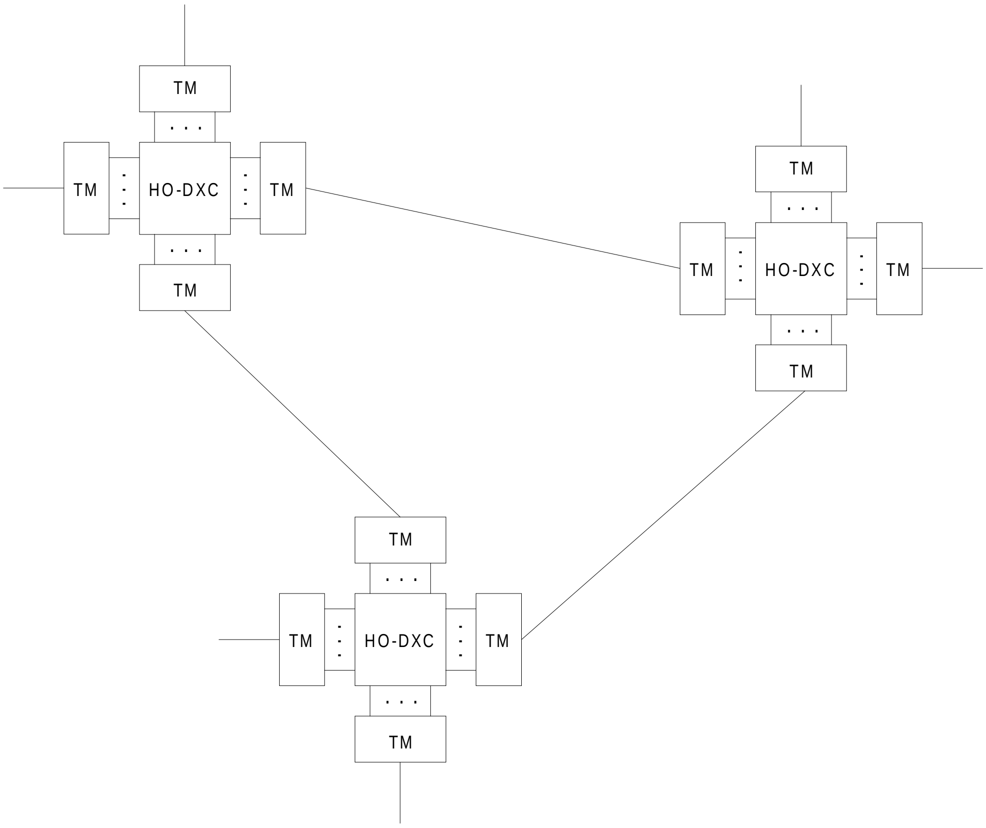


Figure 48: Present structure of core network with HO-DXC and terminal multiplexer

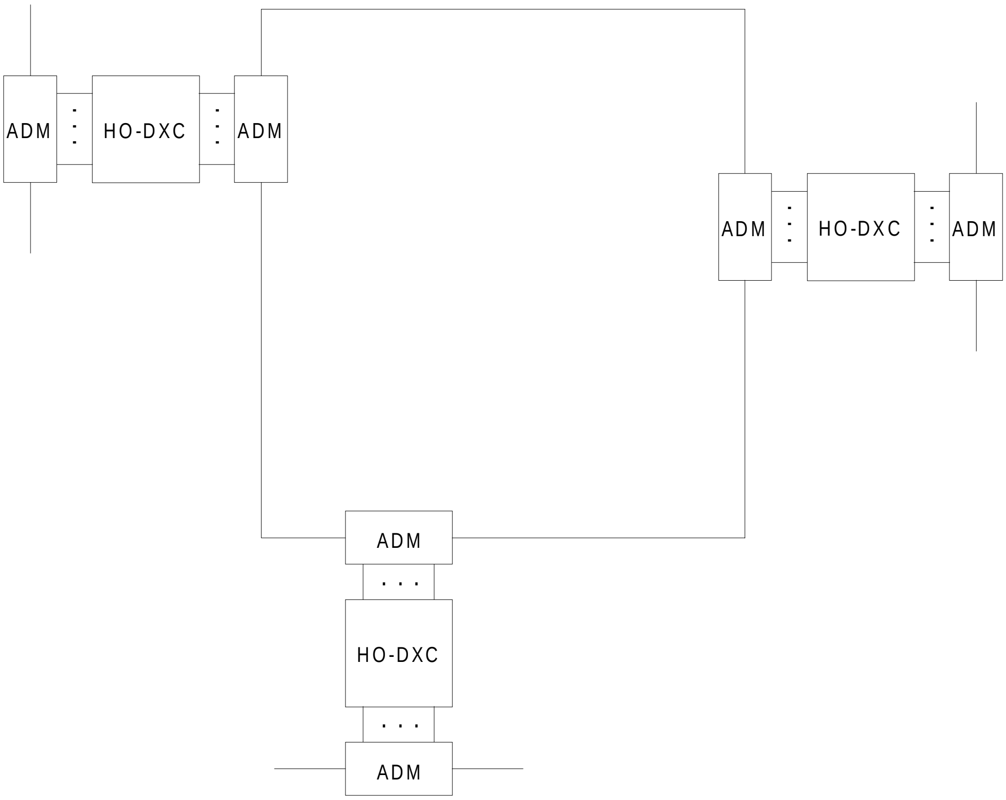


Figure 49: Possible evolution of core network with HO-DXC and MS-SPRings

10.2.2.2 MS-DPRing

This is for further study.

10.2.2.3 VC trail (HO & LO)

VC trail protection is applicable where the VC trail is terminated within the core network.

This is for further study.

10.2.2.4 HO-SNC

The core network is characterized by a uniform traffic pattern between each site. There exists, in addition, different requirements on traffic availability (e.g. leased lines and switched traffic).

With HO SNC protection, it is possible to protect traffic on individual HO VCs. Just the traffic which has to be protected can be protected by HO SNC protection which leads to an efficient bandwidth use in the core network.

HO SNC protection can be implemented as HO SNC/I or HO SNC/N protection. Whereas the HO SNC/I protection protects the HO path against failures in the server layer (MS layer) the HO SNC/N protection protects, in addition, against failures in the HO SNCs (e.g. path misconnection identified by TIM, Signal Degrade).

HO SNC protection works without interaction with a network management system and without any protocol between the network elements. Therefore the HO SNC protection guarantees a simple but efficient protection of HO paths.

The HO SNC protection is applicable for meshed or ring like network topologies. There is no dependence on the topology.

Figure 50 shows a partially meshed network with DXCs providing the HO SNC protection functionality.

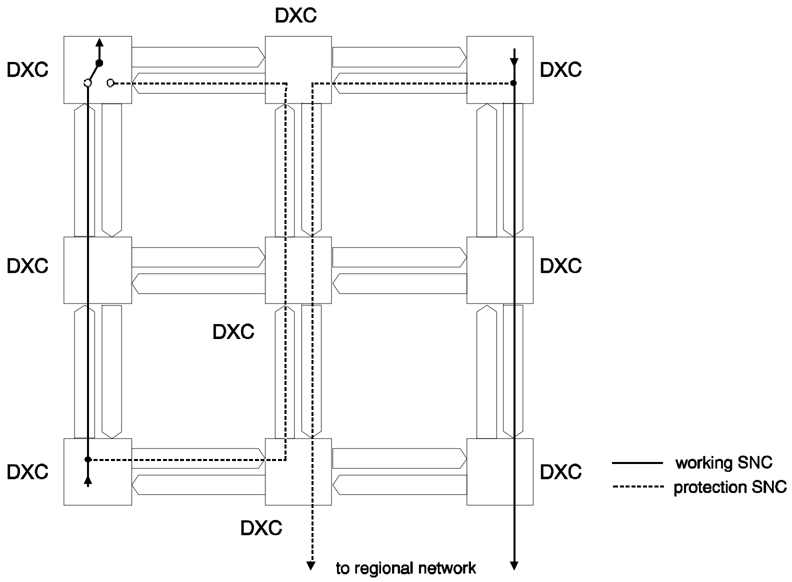


Figure 50: Partially meshed network with DXCs

The HO SNC protection for the VC-4s to be protected can be set up between the DXCs in the core network and again a HO SNC protection could be set up in the served regional network. The VC-4s which do not need protection can be routed as unprotected VC-4s.

It is also possible to extend the HO SNC protection to the served regional network if there is no need for a segmentation of the protection.

In general there are no requirements for having equal value link capacities between the sites. Every mix of link capacities is possible, just the minimum transport capacities between the sites shall be available.

The HO SNC protection in a meshed network gives also the advantage of a simple and smooth extendibility of the network by upgrading link capacities or by adding further links where it is necessary. In addition a high level of flexibility is guaranteed if the traffic pattern or the percentage of VC-4s to be protected will change in the future.

10.2.2.5 LO-SNC

This is normally not applicable because the core is usually managed at the VC4 level. If it is deployed the comments for LO-VC (subclause 10.3.4) apply.

10.3 Access network

10.3.1 Access network characteristics

The SDH access transport network can be characterized as follows:

- lower speeds are predominant, e.g. STM-1 and STM-4;
- traffic patterns are frequently hubbed;
- integrated LO VC access and routeing.

In this part of the network we are dealing with VCs that are contained within a single access transport network as well as VCs that are transferred to other access transport networks via an intermediate network.

Particularly in access networks only part of the traffic may need to be protected. If this is a requirement, then this rules out section layer protection and leads to path layer protection, in particular LO path protection, which offers selectivity.

There are three requirements for protection: the first is to protect paths confined to one access network; the second is to protect paths that transit one or more intermediate networks which may not offer sufficient protection; the third is the provision of dual node interconnection with other networks.

The lower transport speeds (e.g. STM-1, STM-4) present in the access network will normally require management at the LO VC level. From the protection schemes listed in clause 6, only a few schemes are suitable for supporting protection per sub-network. The need to protect per sub-network can come from availability and/or independence objectives. One practical candidate is (S)NC Path Layer Protection. In low speed rings integrated LO VC access will be needed on many occasions.

10.3.2 Protection schemes applied to the access network

10.3.1.1 MS-SPRing

This is for further study.

10.3.2.2 MS-DPRing

This is for further study.

10.3.2.3 VC trail (HO & LO)

Where end to end protection is required the terminations may be located in the access network.

HO protection will not be applicable if the access network is managed at the LO VC level. There may be cases where the access network is managed at the HO VC level (e.g. in a broad-band access network).

A LO/HO path protection ring can be used to provide protection for a customer multiplexer. Two nodes on the ring can serve as dual parents for the customer multiplexer as shown in figure 51. This allows the customer traffic to be protected against failure of either one of the parent SDH multiplexers or the STM-M lines feeding the customer multiplexer. Thus path protection in the STM-N ring can be extended to the customer multiplexer.

The customer multiplexer can also be connected to a single node on the STM-N ring using two STM-M tributaries. This can provide protection for the link to the customer multiplexer but not against a failure of the ring node.

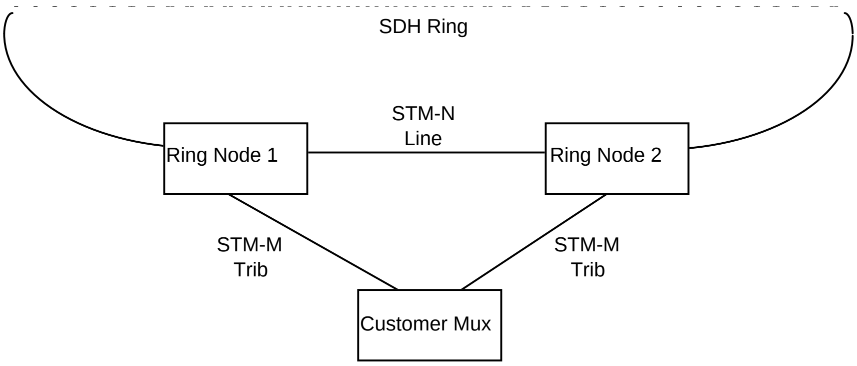


Figure 51: customer multiplexer protected by dual parents

10.3.2.4 HO-SNC

See subclause 10.3.2.3.

10.3.2.5 LO-SNC

See subclause 10.3.2.3.

It is likely that in a transport network end-to-end path layer protection will be applied in some cases and path layer protection per sub-network will be applied in other cases. Compared to end-to-end protection, path protection per sub-network can offer increased availability and better independence. Path layer (S)NC protection can be used as an end-to-end scheme (NC) and for protection per SNC. Trail protection can only be used as an end-to-end scheme.

Where network connections are very long, it may be necessary to partition the protection to protect against multiple failures. SNC allows this partitioning.

11 Summary and conclusions

Table 4: Summary of protection schemes

Protection Type	Architecture	Switching type	Operation type	APS signal	Secondary traffic
VC-m SNC (I&N)	1+1	Single ended	Non-revertive	No	No
VC-m SNC (I&N)	1+1	Single ended	Revertive	No	No
VC-m SNC (I&N)	1+1	Dual ended	For further study		
VC-m SNC (I&N)	1+1	Dual ended	For further study		
VC-m SNC (I&N)	1:1	For further study			
VC-m SNC (I&N)	1:n	For further study			
VC-m Trail	1+1	Single ended	Non-revertive	No	No
VC-m Trail	1+1	Single ended	Revertive	No	No
VC-m Trail	1+1	Dual ended	Non-revertive	Yes	No
VC-m Trail	1+1	Dual ended	Revertive	Yes	No
VC-m Trail	1:1	For further study			
MS Linear	1+1	Dual ended (note)	Non-revertive	Yes	No
MS Linear	1+1	Dual ended (note)	Revertive	Yes	No
MS Linear	1:n	Dual ended	Revertive	Yes	Yes
MS SPRing	Shared	Dual ended	Revertive	Yes	Yes
MS DPRing	1+1	Dual ended	Revertive	Yes	No
MS DPRing	1:1	For further study			
NOTE: Single ended operation of MS Linear protection is possible but is generally not used.					

Comments:

1) no work will be carried out on items listed as "for further study" unless applications are identified;

2) no requirements have been identified for 1:n VC-m trail protection and so this has been omitted from table 4;

3) no work will be carried out on sublayer protection scheme unless applications are identified.

Table 5: Summary of protection scheme attributes

MS Linear:

- linear protection scheme;
- simple implementation;
- can support secondary traffic;
- can generally only cope with a single failure.

MS SPRing:

- ring protection scheme;
- offers advantage in terms of bandwidth efficiency except when the traffic distribution is double hubbed with hub nodes adjacent;
- protocol allows secondary traffic
- best suited to high capacity rings (e.g. STM-16 and above);
- best suited to HO access;
- relatively complicated protocol;
- there is an additional transmission delay under failure conditions.

MS DPRing:

- simple ring protection scheme;
- HO or LO granularity;
- no protocol currently defined for secondary traffic;
- normal mode of operation uses diverse routeing;
- there is an additional transmission delay under failure conditions.

HO/LO SNC (I) protection;

- flexible application to any sub-network;
- simple implementation;
- HO/LO granularity;
- no protocol currently defined for secondary traffic;
- protects against signal failures (in the server layer).

HO/LO SNC (N) protection:

- flexible application to any sub-network;
- Ho/LO granularity;
- no protocol currently defined for secondary traffic;
- protects against signal failures (in the server layer);
- protects against signal failure and signal degradation (in the client layer);
- protects against path mis-connection;
- requires more circuitry than HO/LO SNC (I) protection.

HO/LO VC Trail protection:

- end to end path protection only;
- simple implementation;
- HO/LO granularity;
- can support secondary traffic;
- can generally only cope with a single failure.

In networks where the traffic is predominantly "site to adjacent site", "uniform" or double hubbed with the hub nodes "opposite", then MS SPRings can provide superior capacity utilization compared to MS DPRings or LO/HO path protection schemes.

In networks where the traffic is predominantly single hubbed or double hubbed with the hub nodes adjacent, then MS DPRings or LO/HO path protection rings are more appropriate.

MS trail shared protection networks only have real benefit for a line rate of STM-16 as there are insufficient AU-4s in the multiplexer section at STM-4 to give any benefit and the technique cannot be applied to networks with a line rate of STM-1. LO/HO protection is valid over all trails and line rates and can be used in all topologies where two independent trails exist.

Annex A (informative): Derivation of the maximum number of nodes of MS rings

This annex gives some basic formulas to calculate the capacity of a ring and then derives the maximum number of nodes which can be connected in a ring as a function of the capacity and the granularity of the ring itself.

A.1 General concept

This annex considers the MS SPRings and the MS DPRings. The analysis takes into account the four traffic distributions which are defined in the main body of this present document:

- site to adjacent site;
- uniform;
- single hub;
- double hub.

Between any two given nodes a certain traffic relationship exists. In this analysis the following definitions are used:

d = traffic demand between any two sites;

n = number of nodes in a ring.

As MS SDH rings are considered, the traffic demand d is intended as the number of VC between the two given nodes. To simplify the analysis, the type of the VC (VC-12, VC-4,...) between the nodes is supposed to be the same for every node in the ring.

The capacity could be defined as the maximum number of VCs which should be carried over the largest span on the ring. Capacity depends on traffic distribution, number of nodes and granularity of the ring.

A.2 MS DPRing

In a ring with uniform routeing, all traffic is routed through all spans in only one direction. Each span carries all traffic around the ring and then the capacity requirement is the sum of all traffic demand on the ring. Indicating with n_c the number of pairs of nodes which have traffic relationship, the capacity is:

$$C = n_C d$$

The number of pairs of nodes is derived from the traffic distribution and from geometrical property of polygons.

The maximum number of node is obtained from the capacity formula calculating the number of node n for a given capacity of the ring.

A.2.1 Site to adjacent site traffic distribution

The total number of pairs of adjacent sites is n, then the required capacity is:

$$C = nd$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{\mathrm{C}}{d}$$

A.2.2 Uniform traffic distribution

The total number of pairs of sites is the number of couple in a set of n elements, that is n (n-1)/2. Then the required capacity is:

$$C = \frac{n(n-1)d}{2}$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{1 + \sqrt{1 + \frac{8C}{d}}}{2}$$

A.2.3 Single hub traffic distribution

As n-1 nodes are connected to a single hub, the total number of pairs of sites is n-1. Then the required capacity is:

$$C = (n-1)d$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C}{d} + 1$$

A.2.4 Double hub traffic distribution

In the double hub distribution, all the nodes have a traffic demands d directed towards each of the two hubs.

As n-2 nodes are connected each of 2 hubs the total number of pairs of sites is 2(n-2). Then the required capacity is:

$$C = 2(n-2)d$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C}{2d} + 2$$

A.3 MS SPRing

In a ring with uniform routeing the traffic carried over a given span is not equal for each span, but depends on the traffic distribution. In a MS SPRing the capacity is divided in two half, one for protection, then the capacity requirement is twice the number of traffic demand carried on the largest span.

A.3.1 Site to adjacent site traffic distribution

Each span carries a traffic demand d between a pair of adjacent nodes, then the required capacity is:

$$C = 2d$$

As the capacity is independent from n, the maximum number of nodes on the ring does not depend on the capacity of the ring and is only restricted to 16 by the addressing capability of the APS protocol.

A.3.2 Uniform traffic distribution

Three different cases have to be considered:

- rings with odd number of sites (n odd);
- rings with even number of sites (n even) and even traffic demand (d even);
- rings with even number of sites (n even) and odd traffic demand (d odd).

This is due to the fact in evaluating the required capacity, odd-site rings do not involve splitting of traffic demands, while even-site rings involve some splitting of traffic demands. When the traffic demand between two nodes is split into two different routes along the ring, the split is d/2 and d/2 for d even and is (d+1)/2 for d even and (d-1)/2 for d odd.

A.3.2.1 Odd-site ring

No traffic splitting is involved. Based on the geometric property of a polygon, the required capacity is:

$$C = \frac{(n^2 - 1)d}{4}$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \sqrt{\frac{4C}{d} + 1}$$

A.3.2.2 Even-site ring and even traffic demand between nodes

The traffic demand between two nodes located in opposite points on the ring can be split in two parts of size d/2. Based on the geometric property of the polygons, the required capacity is:

$$C = \frac{n^2 d}{4}$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \sqrt{\frac{4C}{d}}$$

A.3.2.3 Even-site ring and odd traffic demand between nodes

The traffic demand between two nodes located in opposite points on the ring can be split in two parts of size (d+1)/2 and (d-1)/2. This would require complex analysis in order to evaluate the largest span. To simplify the analysis the worst case can be taken, that is all the split traffic contribution to the largest span are of size (d+1)/2. Based on this assumption, the required capacity is:

$$C = \frac{n^2 d}{4} + \frac{n}{2}$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{-1 + \sqrt{1 + 4Cd}}{d}$$

A.3.3 Single hub traffic distribution

Also for this traffic distribution, three different cases have to be considered:

- rings with odd number of sites (n odd);
- rings with even number of sites (n even) and even traffic demand (d even);
- rings with even number of sites (n even) and odd traffic demand (d odd).

This is due to the fact in evaluating the required capacity, odd-site rings do not involve splitting of traffic demands, while even-site rings involve some splitting of traffic demands. When the traffic demand between two nodes is split into two different routes along the ring, the split is d/2 and d/2 for d even and is (d+1)/2 and (d-1)/2 for d odd.

A.3.3.1 Odd - site ring

No traffic splitting is involved. Based on the geometric property of a polygon, the required capacity is:

$$C = (n-1)d$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C}{d} + 1$$

A.3.3.2 Even-site ring and even traffic demand between nodes

The traffic demand of the node located opposite to the hub (the node which has the largest number of spans to reach the hub) can be split in two parts of size d/2. Based on the geometric property of the polygons, the required capacity is:

$$C = (n-1)d$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C}{d} + 1$$

A.3.3.3 Even - site ring and odd traffic demand between nodes

The traffic demand of the node located opposite to the hub can be split in two parts of size (d+1)/2 and (d-1)/2. The largest span is the span adjacent to the hub that supports the (d-1)/2 splitting traffic demand. Then the required capacity is:

$$C = (n-1)d + 1$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C-1}{d} + 1$$

A.3.4 Double hub traffic distribution

In the double hub distribution, all the nodes have a traffic demand (d) directed towards each of the two hubs.

NOTE: It is assumed that there is no traffic between the two hub nodes as defined in subclause 4.4.2.

The required capacity depends on the relative position of the two hubs on the ring. The worst case is when the two hubs are adjacent, then the largest spans are the two spans adjacent to the hubs, but not the span between the hubs themselves. Two cases are considered below:

i) where the two hub nodes are adjacent (subclause A.3.4.1); and

ii) when the two hub nodes are "opposite", e.g. as far apart as possible (subclause A.3.4.2).

A.3.4.1 Hub nodes adjacent

If the number of sites n is odd, no splitting of traffic demand is required, while, if n is even some splitting of traffic demands is possible but, due to the symmetry of the ring, the splitting of traffic demands does not reduce the required capacity. Due to geometric property of the polygons, the required capacity results the same in both cases and is:

$$C = 2(n-2)d$$

From the previous formula, the maximum number of nodes is:

$$n_{\max} = \frac{C}{2d} + 2$$

A.3.4.2 Hub nodes "opposite"

This subclause gives the formulae for a dual hub traffic pattern where the nodes are "opposite". Again it is assumed that there is no traffic between the two hub nodes.

Let us assume an even number of nodes, and the two hub nodes as far apart as possible. The ring is split in two halves with the hub nodes in the middle of the ring, on opposite sides. One can see that the maximum amount of traffic on a link to one of the hubs is determined by only one half of the ring. The situation is identical to a network with half of the number of non-hub nodes (n'=(n-2)/2+2), and two adjacent hub nodes. The formula for this is C=2(n-2)d. This becomes C=2((n-2)/2+2-2)d=(n-2)d. So the capacity needed is only half for an even number of nodes, if the hub nodes are on opposite sides of the ring in stead of adjacent on the ring.

If the number of nodes is odd, the capacity needed is equal to that of the next number of even nodes. So the formula becomes C=(n-1)d for an odd number of nodes and the hubs as far apart as possible.

The formulae for the maximum number of nodes for rings with an even number of nodes is:

$$n_{\max} = \frac{C}{d} + 2$$

The formulae for the maximum number of nodes for rings with an odd number of nodes is:

$$n_{\max} = \frac{C}{d} + 1$$

A.4 Comparison for AU-4 granularity

Using the formulas derived in the previous subclauses it is possible to evaluate the maximum number of nodes for an MS ring of a given capacity.

In table A.1 is shown a comparison between an MS DPRing and a MS SPRing of the same capacity. Both the rings have two fibres and AU-4 granularity. Two different SDH hierarchical levels are considered: STM - 4 equivalent to a capacity of 4 AU - 4, and STM-16, equivalent to a capacity of 16 AU-4. The traffic demand d is equal to one VC-4.

Table A.1: Maximum number of nodes for MS nodes for MS DPRings and two fibre MS SPRings

	MS DPRing		**MS SPRing**	
	STM-4	STM-16	STM-4	STM-16
Site to adjacent site	4	16	∞ (note)	∞ (note)
Uniform	3	6	3	7
Single hub	5	17 (note)	5	17 (note)
Double hub (hub nodes adjacent)	4	10	4	10
Double hub (hub nodes opposite)	4	10	6	18 (note)
NOTE: The maximum number of nodes may be limited by the APS protocol.				

To show how the values in the table A.1 have been calculated, an example in the case of uniform traffic distribution for an STM-4 MS SPRing can be considered.

The capacity of the ring is:

$$C = 4$$

and the traffic demand is:

$$d = 1$$

Making the assumption that n is odd:

$$n = \sqrt{(\frac{4C}{d} + 1)} = 4{,}12$$

and the largest odd value of n that satisfies the relation is:

$$n = 3$$

Making the assumption that n is even:

$$n = \frac{-1 + \sqrt{1 + 4Cd}}{d} = 3{,}12$$

and the largest even value of n that satisfies the relation is:

$$n = 2$$

As the maximum number of nodes is looked for, it follows that:

$$n_{\max} = 3$$

Although the capacity is quantized by the hierarchical levels of SDH, the previous table shows that MS SPRings have some advantages over MS DPRings in the cases of site to adjacent site, uniform and double hubbed with hub nodes opposite traffic patterns.

A.5 Pictorial description of the maximum number of nodes in a STM-16 ring with VC-4 granularity and for uniform and double hub traffic patterns

i) Uniform traffic pattern, MS DPRing, STM-16 ring, VC-4 granularity:

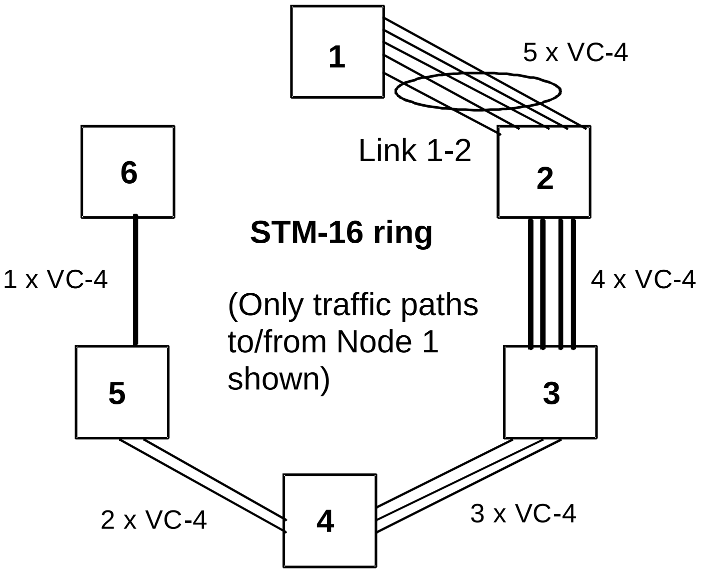


Figure A.1: Pictorial representation of VC-4s to/from Node 1 for uniform traffic pattern, MS DPRing, STM-16 ring, VC-4 granularity

Traffic over section 1-2:

- 5 x VC-4 from Node 1 to Nodes 2,3,4,5,6 (condition shown in figure A.1);
- + 4 x VC-4 from Node 6 to Nodes 2,3,4,5;
- + 3 x VC-4 from Node 5 to Nodes 2,3,4;
- + 2 x VC-4 from Node 4 to Nodes 2,3;
- + 1 x VC-4 from Node 3 to Node 2.

Total traffic over link 1-2 = 5+4+3+2+1 = 15 x VC-4.

The same argument applies to each link.

NOTE 1: If the ring had seven nodes the traffic over each link would be:

6+5+4+3+2+1 = 21 x VC-4,

which is greater than the transmission capacity.

Hence the maximum number of nodes is six and the maximum ring capacity is 15 x VC-4.

ii) Uniform traffic pattern, MS SPRing, STM-16 ring, VC-4 granularity:

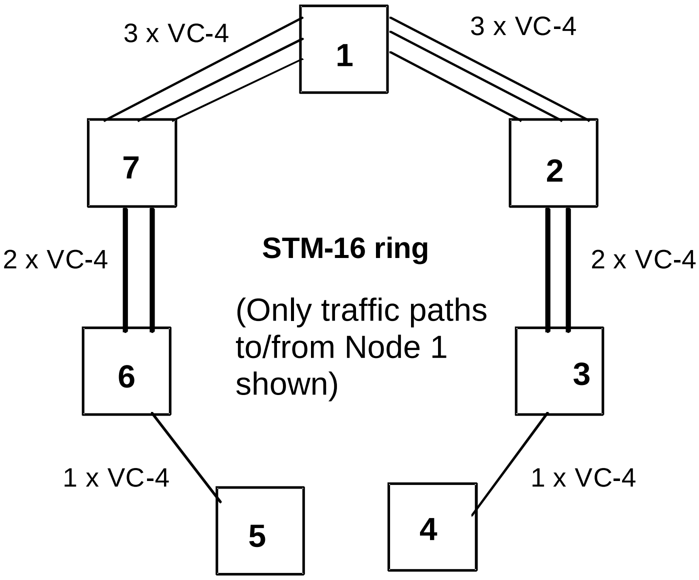


Figure A.2: Pictorial representation of VC-4s to/from Node 1 for uniform traffic pattern, MS SPRing, STM-16 ring, VC-4 granularity

Traffic over section 1-2:

- 3 x VC-4 from Node 1 to Nodes 2,3,4 (Condition shown in figure A.2);
- + 2 x VC-4 from Node 7 to Nodes 2,3;
- + 1 x VC-4 from Node 6 to Node 2;
- + 3 x VC-4 from Node 2 to Nodes 1,7,6;
- + 2 x VC-4 from Node 3 to Nodes 1,7;
- + 1 x VC-4 from Node 4 to Node 1.

Total traffic over Link 1-2 = 12 x VC-4.

The same argument applies to each link.

NOTE 2: If the ring had eight nodes the traffic over each link would be 19 x VC-4 which would be greater than the transmission capacity.

Hence the maximum number of nodes is seven and the maximum ring capacity is 12 x VC-4.

iii) Double hub traffic pattern, MS DPRing, STM-16 ring, VC-4 granularity:

NOTE 3: It is assumed that there is no traffic between the two hub nodes as defined in subclause 4.4.2.

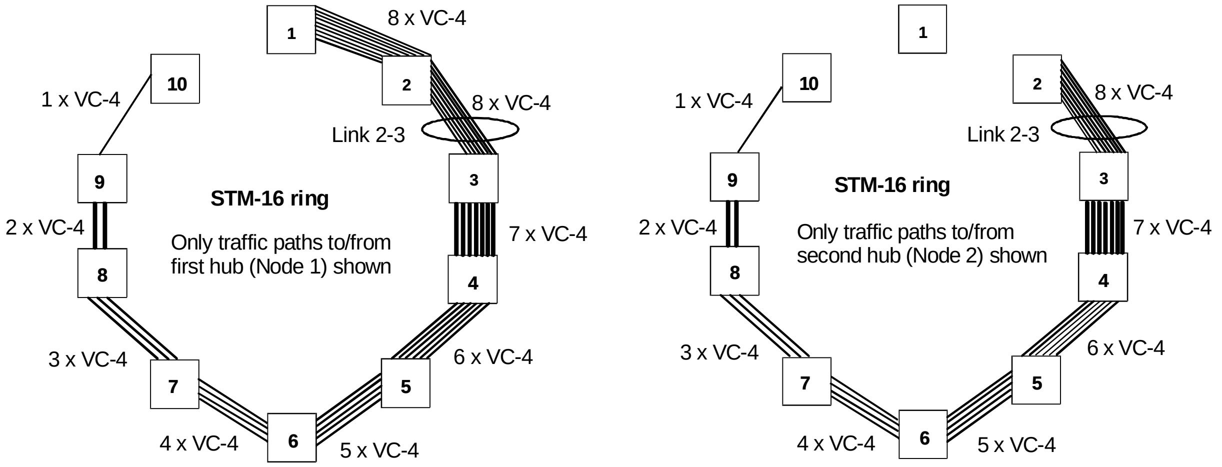


Figure A.3: Pictorial representation of VC-4s to/from Node 1 for a double hub traffic pattern, where the hubs are adjacent MS DPRing, STM-16 ring, VC-4 granularity

For a double hub traffic distribution, the maximum capacity is required on the link adjacent to the hub nodes.

Assuming the hub nodes are Nodes 1 and 2 as shown in figure A.3, then the maximum traffic capacity will be on Link 2-3 (and Link 1-10 for the protection channels routed in the opposite direction around the ring).

For Link 2-3, consider the traffic from Hub Node 1:

8 x VC-4 from Node 1 to Nodes 3,4,5,6,7,8,9,10;

Now consider the traffic from Hub Node 2:

8 x VC-4 from Hub Node 2 to Nodes 3,4,5,6,7,8,9,10.

NOTE 4: Traffic from Node 2 to Node 1 = Traffic from Node 1 to Node 2 and this is included in the traffic from Hub Node 1 above.

Hence the maximum traffic over Link 2-3 = 16 x VC-4.

NOTE 5: If the ring had 11 nodes, the traffic over each link would be: 18 x VC-4 which is greater than the transmission capacity of the ring.

Hence the maximum number of nodes is 10 and the maximum traffic capacity is 16 x VC-4.

iv) Double hub traffic pattern, MS SPRing, STM-16 ring, VC-4 granularity:

NOTE 6: It is assumed that there is no traffic between the two hub nodes as defined in subclause 4.4.2.

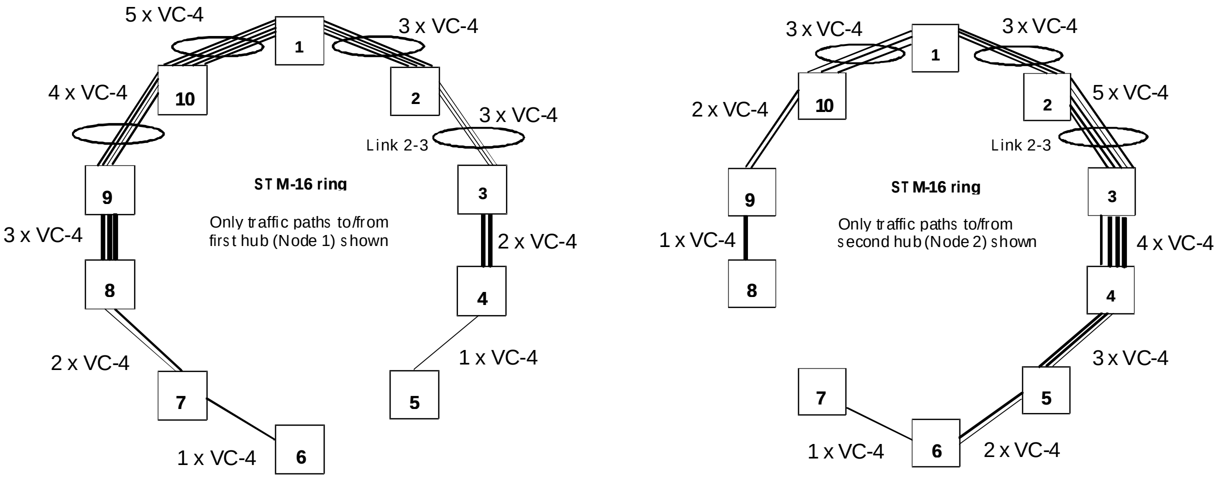


Figure A.4: Pictorial representation of VC-4s to/from Node 1 for a double hub traffic pattern, where the hubs are adjacent MS SPRing, STM-16 ring, VC-4 granularity

For a double hub traffic distribution, the maximum capacity is required on the link adjacent to the hub nodes.

Assuming the hub nodes are Nodes 1 and 2 as shown in figure A.4, then the maximum traffic capacity will be on links 2-3 and 1-10.

For Link 2-3, consider the traffic from Hub Node 1:

3 x VC-4 from Node 1 to Nodes 3,4,5.

NOTE 7: To balance the traffic, 5 x VC-4s are routed in a clockwise direction around the ring and 3 x VC-4s are routed anti-clockwise.

Now consider the traffic from Hub Node 2:

5 x VC-4 from Node 2 to Nodes 3,4,5,6,7.

NOTE 8: Traffic from Node 2 to Node 1 = Traffic from Node 1 to Node 2 and this is included in the traffic from Hub Node 1 above.

Hence the maximum traffic over link 2-3 = 8 x VC-4 in each direction (Total 16 x VC-4).

NOTE 9: If the ring had 11 nodes, the traffic capacity over Link 2-3 would be 18 x VC-4 which is greater than the transmission capacity.

Hence the maximum number of nodes is 10 and the maximum traffic capacity is 16 x VC-4.

Annex B (informative): Use of SNC protection inside a tandem connection sublayer

Figure B.1 shows a scenario where a SNCP/N has been set up inside a tandem connection sublayer. When an incoming AU-AIS condition exist at the Tandem Connection Termination (TCT) source function, due to a failure outside the tandem connection sublayer, the TCT source replaces the AU-AIS condition with a valid pointer value plus a VC-AIS condition.

The VC-AIS is generated by a TCT function when it detects an incoming AU-AIS (or TU-AIS) condition, because the tandem connection sublayer needs to re-generate a valid pointer in order to be able to identify the N1 (or N2) byte, which transports the overhead associated with the tandem connection. The VC-AIS condition can be detected by a Trail Termination supervision (TTs) function as an all ones code in the signal label. The detection of a VC-AIS condition by a TTs results in the activation of the Trail Signal Fail (TSF) condition.

The VC-AIS exists only inside a tandem connection sublayer, because the TCT sink function is responsible to regenerate the AU-AIS (or TU-AIS) condition on the signal leaving the sublayer.

In the scenario of figure B.1, the VC-AIS condition is detected by both the TTs on the SNCP/N forcing both the working and the protection SNCs in a TSF condition. These TSF conditions then prevent any switching possibility inside the protected sub-network.

Now, if a failure occurs on the working SNC, the protection switch will not take place due to the presence of the TSF condition on the two SNCs. This will not affect the traffic that is already lost due to some failure outside the tandem connection but causes the TCT sink functions to declare a tandem connection fail condition even if the failure could have been restored by the SNCP/N.

From a network modelling point of view this is because the SNCP/N protects the HO or LO VC layer and not the tandem connection sublayer. To protect the tandem connection sublayer the SNCP should use two tandem connection supervision functions and make the switch based on defect detected on the tandem connection overhead. This type of protection scheme is not currently defined.

The only way to overcome this problem is to use an SNCP/I scheme, which uses only the SSF condition as a switching criteria. Of course this scheme does not detect a trace identifier mismatch or an UNEQuipped defect generated inside the protected sub-network, but it can guarantee the survivability of the tandem connection to the server layer defects.

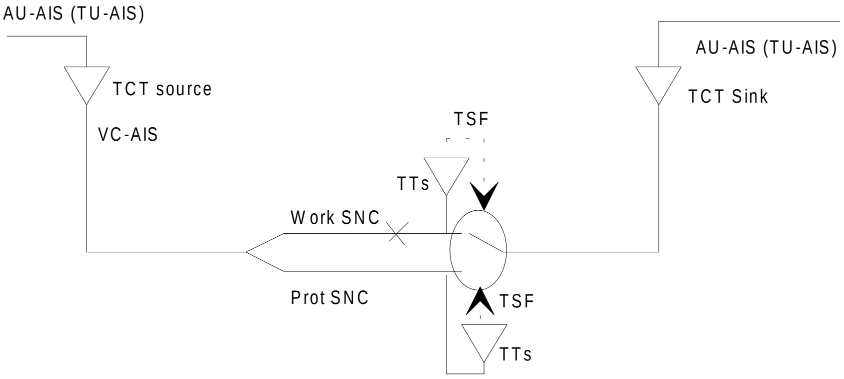


Figure B.1: A SNCP/N inside a tandem connection sublayer

Annex C (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 networks".

- ETS 300 462: "Transmission and Multiplexing (TM); Generic requirements for synchronization networks".

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

History

Document history		
V1.1.1	November 1997	Publication

ISBN 2-7437-0795-X
Dépôt légal : Novembre 1997