INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

I.630

(02/99)

SERIES I: INTEGRATED SERVICES DIGITAL NETWORK

Maintenance principles

ATM protection switching

ITU-T Recommendation I.630

(Previously CCITT Recommendation)

ITU-T I-SERIES RECOMMENDATIONS

INTEGRATED SERVICES DIGITAL NETWORK

GENERAL STRUCTURE	
Terminology	I.110–I.119
Description of ISDNs	I.120–I.129
General modelling methods	I.130–I.139
Telecommunication network and service attributes	I.140–I.149
General description of asynchronous transfer mode	I.150–I.199
SERVICE CAPABILITIES	
Scope	I.200–I.209
General aspects of services in ISDN	I.210–I.219
Common aspects of services in the ISDN	I.220–I.229
Bearer services supported by an ISDN	I.230–I.239
Teleservices supported by an ISDN	I.240–I.249
Supplementary services in ISDN	I.250–I.299
OVERALL NETWORK ASPECTS AND FUNCTIONS	
Network functional principles	I.310–I.319
Reference models	I.320–I.329
Numbering, addressing and routing	I.330–I.339
Connection types	I.340–I.349
Performance objectives	I.350–I.359
Protocol layer requirements	I.360–I.369
General network requirements and functions	I.370–I.399
ISDN USER-NETWORK INTERFACES	
Application of I-series Recommendations to ISDN user-network interfaces	I.420–I.429
Layer 1 Recommendations	I.430–I.439
Layer 2 Recommendations	I.440–I.449
Layer 3 Recommendations	I.450–I.459
Multiplexing, rate adaption and support of existing interfaces	I.460–I.469
Aspects of ISDN affecting terminal requirements	I.470–I.499
INTERNETWORK INTERFACES	I.500–I.599
MAINTENANCE PRINCIPLES	**I.600–I.699**
B-ISDN EQUIPMENT ASPECTS	
ATM equipment	I.730–I.739
Transport functions	I.740–I.749
Management of ATM equipment	I.750–I.799

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

ITU-T RECOMMENDATION I.630

ATM PROTECTION SWITCHING

Summary

This Recommendation "ATM Protection Switching" provides architectures and mechanisms for protection switching at ATM layer. The architecture includes the extent of the protected domain and arrangement of protected domain. The resource for protection entities is pre-allocated. The mechanism includes protection switching trigger, hold-off mechanisms and protection switching control protocol.

This Recommendation describes individual VP/VC protection and group protection. The individual VP/VC protection is a technique where a single network and/or subnetwork connection is used for working entity and protection entity. The group protection is a technique where a logical bundle of one or more network and/or subnetwork connections is used for working entity and protection entity.

Currently, this Recommendation describes 1+1 and 1:1 bidirectional protection switching as well as 1+1 unidirectional protection switching.

Source

ITU-T Recommendation I.630 was prepared by ITU-T Study Group 13 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 26th of February 1999.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

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

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

Recommendation I.630

ATM PROTECTION SWITCHING

(Geneva, 1999)

1 Scope

This Recommendation provides architectures and mechanisms of ATM VP/VC protection switching and ATM VP group protection switching. The architecture includes the extent of the protected domain, arrangement of protected domain, and resource allocation policies. The mechanism includes protection switching trigger, hold-off mechanisms and protection switching control protocol. The modelling methodology defined in Recommendations G.805 [2] and I.326 [4] is used for describing the ATM VP/VC protection switching architecture and ATM VP/VC group protection switching architecture given in this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy, (SDH).*

[2] ITU-T Recommendation G.805 (1995), *Generic functional architecture of transport networks*.

[3] ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures.*

[4] ITU-T Recommendation I.326 (1995), *Functional architecture of transport networks based on ATM*.

[5] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions.*

[6] ITU-T Recommendation I.732 (1996), *Functional characteristics of ATM equipment.*

[7] CCITT Recommendation M.495 (1988), *Transmission restoration and transmission route diversity: terminology and general principles.*

[8] ITU-T Recommendation M.3010 (1996), *Principles for a telecommunications management network.*

[9] ITU-T Recommendation M.3300 (1998), *TMN F interface requirements.*

3 Definitions

This Recommendation defines the following terms:

3.1 APS VCC: A VCC for control purposes, defined over the extent of the protected domain and contained within a VCG. Its purpose is to assist in the evaluation of the quality of the associated VCG and to serve as a conduit for protection switching control protocol messages. There is an APS VCC associated with each VCG_W and an APS VCC associated with each VCG_P. The transmission of protection switching control protocol messages is always over the VCG_P APS VCC.

3.2 APS VPC: A VPC for control purposes, defined over the extent of the protected domain and contained within a VPG. Its purpose is to assist in the evaluation of the quality of the associated VPG and to serve as a conduit for protection switching control protocol messages. There is an APS VPC associated with each VPG_W and an APS VPC associated with each VPG_P. The transmission of protection switching control protocol messages is always over the VPG_P APS VPC.

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

3.4 bridge: (For 1+1 configuration) The action or function of transmitting identical traffic on both the working and protection entities. (For 1:n configuration) To be defined.

3.5 Connection Point (CP): (See Note 2 in 3.38.) Reference points which are defined along a network connection defined at a given network layer. CPs defined at the ATM layer along a VP (or VC) connection are located at the ingress and egress of an ATM network element (or customer equipment), where VP (or VC) link termination functions operate.

3.6 dedicated protection resource allocation: A resource allocation policy where both the route and the bandwidth for the protection entity are pre-allocated.

3.7 egress: The egress point of an ATM network element is illustrated in Figure 1.

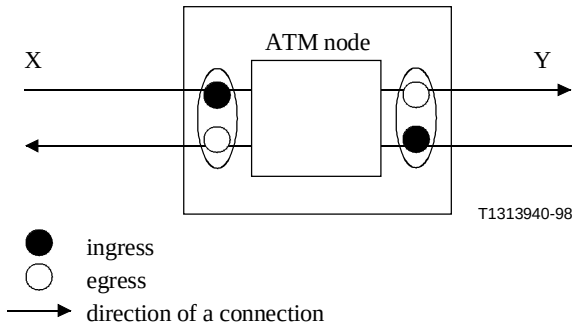


Figure 1/I.630 – Usage of ingress and egress terms in Recommendation I.630

3.8 escalation: A network survivability action caused when the survivability function in lower layers has not been carried out.

3.9 extra traffic: A lower priority traffic with respect to the one being carried by the working entity. It is carried over the protection entity while the working entity is active. The extra traffic is not protected, i.e. when the protection entity is required to protect the traffic that is being carried over the working entity (due to a failure or forced switch/manual switch operation in this last one), the extra traffic is pre-empted.

3.10 forced switch for working entity #n: A switch action initiated by an operator command. Switch action is conducted except when signal fail condition exists for the protection entity to switch over.

3.11 hitless protection switch: A protection switch which does not cause cell loss, cell duplication, cell disorder, or bit errors upon protection switching action.

3.12 hold-off time: The time interval between the detection of an SF or SD and its confirmation as a condition requiring the protection switching procedure.

3.13 impairment: A defect or performance degradation which may lead to SF or SD trigger.

3.14 ingress: The ingress point of an ATM network element is illustrated in Figure 1.

3.15 intermediate node: A node on either the working entity physical route or the protection entity physical route in between the source and sink of the corresponding protected domain.

3.16 link connection: Definition is provided in Recommendation G.805. As an example a VP link connection is delimited by the CPs located in two consecutive ATM network elements operating at VP level.

3.17 manual switch: A switch action initiated by an operator command. Switch action is conducted unless a higher priority request is in effect.

3.18 matrix connection: Subnetwork connection delimited, for the ATM layer, by the CPs located at the ingress and egress of an ATM network element (see Note 2 in 3.38).

3.19 network connection: Transport entity used for transferring user and OAM information between the endpoints of the connection (TCPs) (see Note 2 in 3.38).

3.20 network survivability: The set of capabilities that allow a network to restore affected traffic in the event of a failure. The degree of survivability is determined by the network's capability to survive single failures, multiple failures, and equipment failures.

3.21 non-revertive protection switching: A protection switching method where revertive action (switch back to the working entity) is not taken after the working entity is repaired.

3.22 protected domain for the ATM layer: The protected domain defines one or more VPCs/VCCs, or a portion of this or these connection(s), for which a survivability mechanism is provided in the event of an impairment affecting that or those connections. It begins after the selector/bridge of one endpoint and extends up to the selector/bridge of the other endpoint. It excludes both selector/bridge functions.

3.23 protection entity: The portion of the ATM VPC/VCC or VPG/VCG within the protected domain from which working traffic is received at the sink of the protected domain where a working entity has failed.

3.24 protection switching: A network survivability technique with dedicated protection resource allocation policy.

3.25 revertive protection switching: A protection switching method where revertive action (switch back to the working entity) is taken after the working entity is repaired.

3.26 selector: A switch which selects the traffic from the working entity or the protection entity.

3.27 subnetwork connection: A transport entity corresponding to a part of a network connection. A subnetwork connection can be subdivided into a concatenation of links and matrix connections. As a special case, a matrix connection corresponds to a single (indivisible) subnetwork connection (see Note 2 in 3.38).

3.28 Termination Connection Point (TCP): Endpoints of a network connection (see Note 2 in 3.38).

3.29 trail: A "transport entity" which consists of an associated pair of "unidirectional trails" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs (see Note 2 in 3.38).

3.30 transport entity: An architectural component which transfers information between its inputs and outputs within a layer network (see Note 2 in 3.38).

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

3.32 VCG_P: An alternate physically diverse VCG consisting of protection VC network connections or subnetwork connections assigned to a VCG_W or a set of VCG_Ws (as in 1:n operation).

3.33 VCG_W: A VCG consisting of working ATM VC network connections or subnetwork connections that bear protected traffic in normal, operating conditions.

3.34 virtual channel group (VCG): A logical bundle of one or more ATM VC network and/or subnetwork connections that share the same paths(s) within the protected domain.

3.35 virtual path group (VPG): A logical bundle of one or more ATM VP network and/or subnetwork connections that share the same transmission paths(s) within the protected domain.

3.36 VPG_P: An alternate physically diverse VPG consisting of protection VP network connections or subnetwork connections assigned to a VPG_W or a set of VPG_Ws (as in 1:n operation).

3.37 VPG_W: A VPG consisting of working ATM VP network connections or subnetwork connections that bear protected traffic in normal, operating conditions.

3.38 working entity: The portion of the ATM VPC/VCC or VPG/VCG within the protected domain from which working traffic is received at the sink of the protected domain under fault-free condition in revertive mode.

NOTE 1 – This function is different from the "bridge" defined in Recommendation G.841 [3].

NOTE 2 – Recommendation G.805 gives a more general and detailed definition.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

AIS	Alarm Indication Signal
AN	Access Network
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
CP	Connection Point
CPN	Customer Premises Network
e-t-e_VC-XX	OAM cell providing the "XX" OAM function for an end-to-end VCC (e.g. e-t-e_VC-AIS ...)

e-t-e_VP-XX	OAM cell providing the "XX" OAM function for an end-to-end VPC (e.g. e-t-e_VP-AIS ...)
e-t-e_XX	OAM cell providing the "XX" OAM function for an end-to-end VPC or VCC (e.g. e-t-e_AIS ...)
MS	Manual Switch
NIM	Non-Intrusive Monitoring
OAM	Operations and Maintenance
PS	Protection Switching
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
seg_VC-XX	OAM cell providing the "XX" OAM function for a VCC segment (e.g. seg_VC-AIS ...)
seg_VP-XX	OAM cell providing the "XX" OAM function for a VPC segment (e.g. seg_VP-AIS ...)
seg_XX	OAM cell providing the "XX" OAM function for a VPC or a VCC segment (e.g. seg_AIS ...)
SF	Signal Fail
SN	Subnetwork
SNC	SubNetwork Connection
TCP	Termination Connection Point
TE	Terminal Equipment
TMN	Telecommunications Management Network
VC	Virtual Channel
VCC	Virtual Channel Connection
VCG	Virtual Channel Group
VCI	Virtual Channel Identifier
VP	Virtual Path
VPC	Virtual Path Connection
VPG	Virtual Path Group
VPI	Virtual Path Identifier

5 Protection switching principles

The individual VP/VC protection switching concept was developed to apply primarily to the situations where a server layer protection switching does not exist. It is useful to protect only a part of VPs/VCs which need high reliability. The rest of the VPs/VCs remain unprotected. This helps to reduce the necessary bandwidth for protection. Although it can be used for protection against ATM layer defects as well as physical layer defects, application for protection against only physical layer defect is not precluded.

The VPG/VCG protection concept was originally developed at the ATM layer to facilitate fast (on the order of SDH layer protection switching completion times) ATM layer protection switching primarily in situations where a server layer protection switching mechanism does not exist or cannot be deployed. Fast protection switching is obtained through the treatment of a logical bundle of VP/VC network and/or subnetwork connections as a single entity of VPG/VCG after the commencement of protection actions. While VPG/VCG protection was devised primarily to recover from physical layer failures, the VPG/VCG protection concept does not preclude its usage in protection against ATM layer defects. Also, VPG/VCG protection could be used in conjunction with individual VP/VC protection switching techniques, which can be used to protect individual VP/VC connections against ATM layer defects.

Protection switching is a fully allocated protection mechanism that can be used on any physical topology. It is fully allocated in the sense that the route and bandwidth of the protection entity is reserved for a selected working entity.

The ATM PS architecture can be a 1+1 type or an *m*:*n* type.

In the 1+1 architecture type, a protection entity is dedicated to each working entity with the working entity bridged onto the protection entity at the source of the protected domain. The traffic on working and protection entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection entity is made based on some predetermined criteria, such as server defect indication.

In the *m*:*n* architecture type, *m* dedicated protection entities are shared by *n* working entities, where $m \leq n$ typically. The bandwidth of each protection entity should be allocated in such a way that it may be possible to protect any of the *n* working entities in case at least one of the *m* protection entities is available. When a working entity is determined to be impaired, it first must be assigned to an available protection entity followed by transition from the working to protection entity at both the source and sink of the protected domain. It is noted that when more than *m* working entities are impaired, only *m* working entities can be protected.

5.1 General principles, requirements and objectives

The following general principles, requirements and objectives are common to VC, VP, VCG and VPG protection switching.

5.1.1 General principles

This subclause provides a list of general principles used to guide ongoing ATM protection architectures and mechanisms development.

1) ATM protection techniques should be applicable to VPG, VP, VCG and VC.
2) Network layering violations should be avoided (e.g. an individual ATM VP level defect should not trigger SDH layer alarms).
3) In general, if lower layer (e.g. SDH or optical) protection mechanisms are being utilized in conjunction with ATM layer protection mechanisms then the lower layers should have a chance to restore working traffic before the ATM layer initiates protection actions. The objective here is to avoid unnecessary protection actions and any issues of contention.
4) Protection switching actions in one protected domain should not adversely affect network operations and performance in other domains.
5) The protection switching mechanism should facilitate fast recovery of working traffic to minimize the network unavailability.

5.1.2 General requirements and objectives

1) Protection for VP/VC trails and subnetwork connections (SNCs).

2) Protection of SNC protected domains that are independent of or aligned with F4 or F5 OAM segment flows (see Recommendation I.610 [5]).

3) Linear, ring, or mesh physical topologies.

4) Signal Fail (SF) and Signal Degrade (SD) detection should be used for triggering protection switching. Trigger for SD is for further study.

5) SF detection times as fast as possible.

6) Prioritized protection for SF, SD, and operator switch requests.

7) Protection switch completion time: the possibility to achieve protection at the ATM layer as fast as possible should be provided. As an example, this could be of great interest in case the physical layer has no means to protect against failures (e.g. case of a ring structure collecting traffic from ATM nodes). The exact value(s) is for further study.

8) Protection ratio of 100%, i.e. 100% of impaired working traffic is protected for a failure on a single working entity.

9) 1+1 unidirectional as well as 1+1, 1:1, bidirectional protection switching modes should be supported (generalized *m*:*n* mode requires further study on the protection resource allocation technique).

10) Extra traffic capability, when possible.

11) Protection switching control protocol based upon SDH APS principles and features to the extent feasible.

12) Inter-layer and intra-layer escalation strategy should be supported.

13) Use existing OAM tools defined in Recommendation I.610 and minimize introduction of new OAM tools to the extent possible.

14) No unintended interference with protection of the physical layer.

15) The combination of individual VP/VC and VPG/VCG protection switching should be possible.

16) Revertive and non-revertive switching should be provided as a network operator option.

17) Operator control such as lockout of protection, forced switch and manual switch commands should be supported.

18) A "generic hold-off function" should be provided so as to delay the beginning of the protection action. The hold-off time achieved by this function should be provisionable by the network operator so as to operate either an "as soon as possible" protection action or to delay this action for several seconds.

19) The ATM layer connectivity of the protection entity should be periodically monitored so as to assure availability when protection switching needs to take place. The insertion frequency of APS cells is one cell per 5 seconds. Provisionable insertion frequency is for further study. The need for further monitoring (e.g. bandwidth, performance, etc.) of the protection entity is for further study.

    NOTE – The insertion frequency was determined by the trade-off between the required bandwidth for APS cells and additional delay when an APS cell is lost.

20) The nested protection should be provided if possible.

21) In the first version of Recommendation I.630, hitless protection switching is not required.

5.2 Examples of network protected domains

Figure 2 illustrates examples of protected domains. The protected domain may extend:

- across a network connection;
- across a subnetwork connection;
- across a single link connection.

The protected domain for VPC/VCC may coincide with the extent of e-t-e or segment OAM flows. Recommendation I.732 [6] defines two types of segment termination functionality. One has the source in front of the matrix and the associated sink behind the matrix. The other has the source behind the matrix and the associated sink in front of the matrix. If the endpoints of the protected domain coincide with segment termination points of the latter type, ATM protection switching mechanisms applied on the protected domain may make use of VPC/VCC segment OAM tools.

When the protected domain does not coincide with the extent of e-t-e or segment OAM flows, capabilities such as non-intrusive monitoring of existing OAM tools may need to be employed for ATM protection switching mechanisms applied on the protected domain.

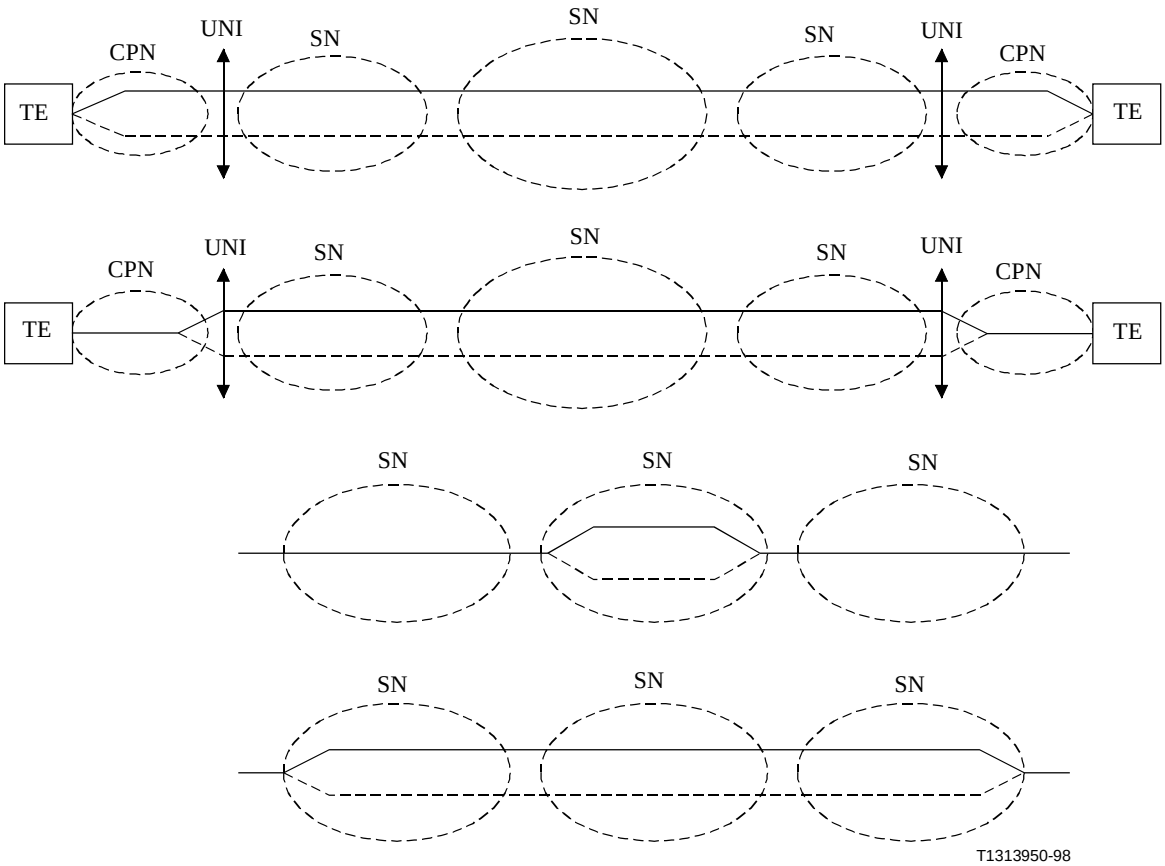


Figure 2/I.630 – Examples of protected domains

5.3 Extent of the protected domain

In the following subclauses, terms below are used:

- 1+1/1:1 trail [e-t-e connection] protection – this scheme uses the e-t-e connection OAM to monitor the trail [e-t-e connection] within the protected domain.

- 1+1/1:1 sublayer monitored subnetwork connection protection (SNC/S) – this scheme requires that extra protection domain or connection supervision segment OAM is added to monitor the subnetwork connection within the protected domain.
- 1+1 non-intrusive monitored subnetwork connection protection (SNC/N) – this scheme does not require extra OAM to be used to monitor the subnetwork connection within the protected domain; it is as such restricted to 1+1 unidirectional. This scheme is applicable for individual VP/VC protection only and not applicable for group protection.
- 1+1/1:1 test trail monitored subnetwork connection protection (SNC/T) – this scheme is applicable for group protection only; an extra test trail (e-t-e connection) is set up between source and sink of the protected domain. The status of this test trail is used as indication of the SF and SD condition of the group.

  NOTE 1 – Test trail for group protection is referred to as an APS VPC/VCC in clause 7.

  NOTE 2 – In the general case, network connections and subnetwork connections carrying user traffic can be assigned to the same group.
- 1+1/1:1 test trail monitored trail protection (trail/T) – this scheme is applicable for group protection only; an extra test trail (e-t-e connection) is set up between source and sink of the protected domain. The status of this test trail is used as indication of the SF and SD condition of the group.

5.3.1 Trail protection

Figure 3 shows an example of 1+1 or 1:1 individual VP/VC trail protection.

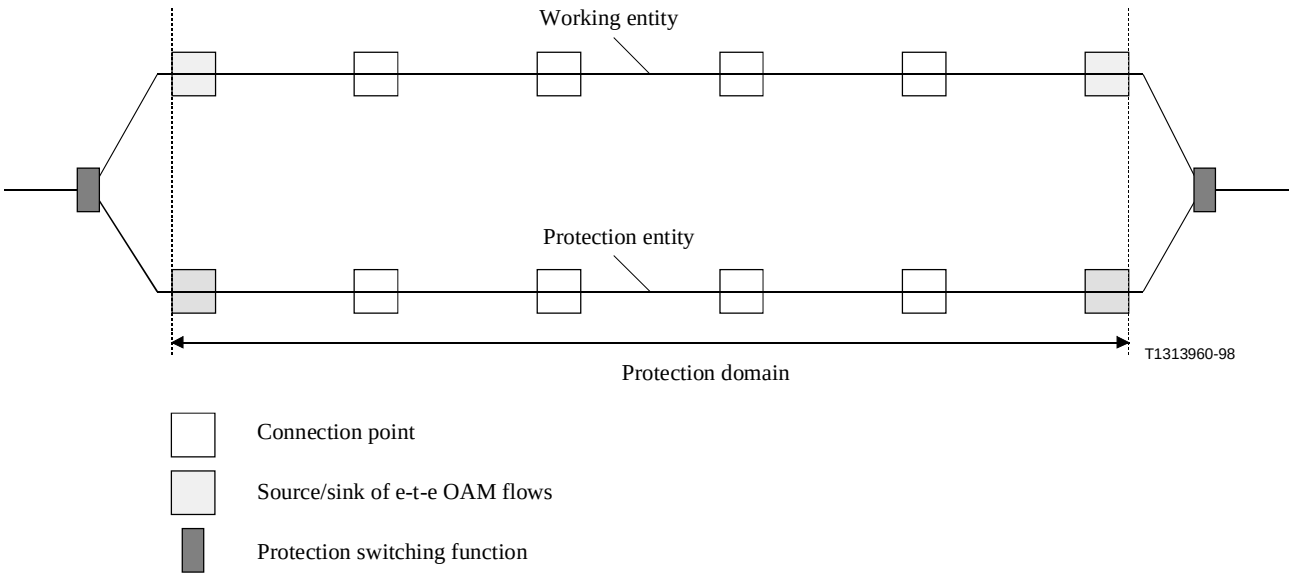


Figure 3/I.630 – 1:1 or 1+1 individual VP/VC trail protection

Figure 4 shows an example of 1+1 or 1:1 trail/T group protection.

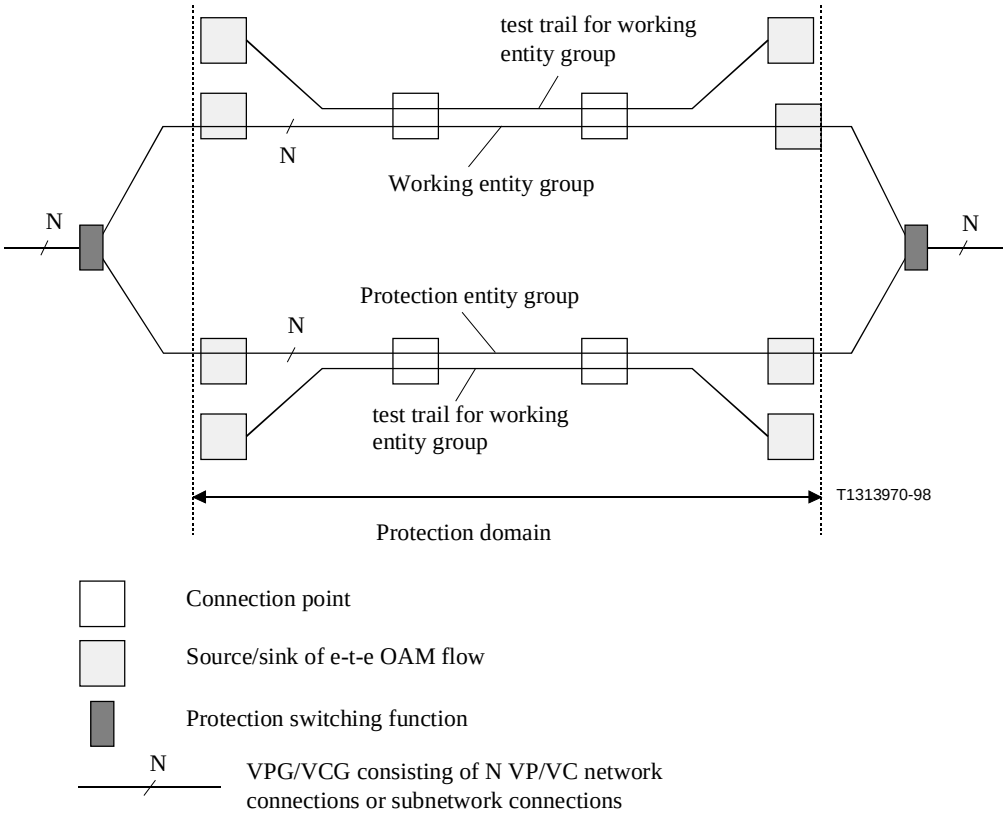


Figure 4/I.630 – 1+1 or 1:1 trail/T group protection

5.3.2 Subnetwork connection protection

Figure 5 shows an example of 1+1 or 1:1 SNC/S individual VP/VC protection.

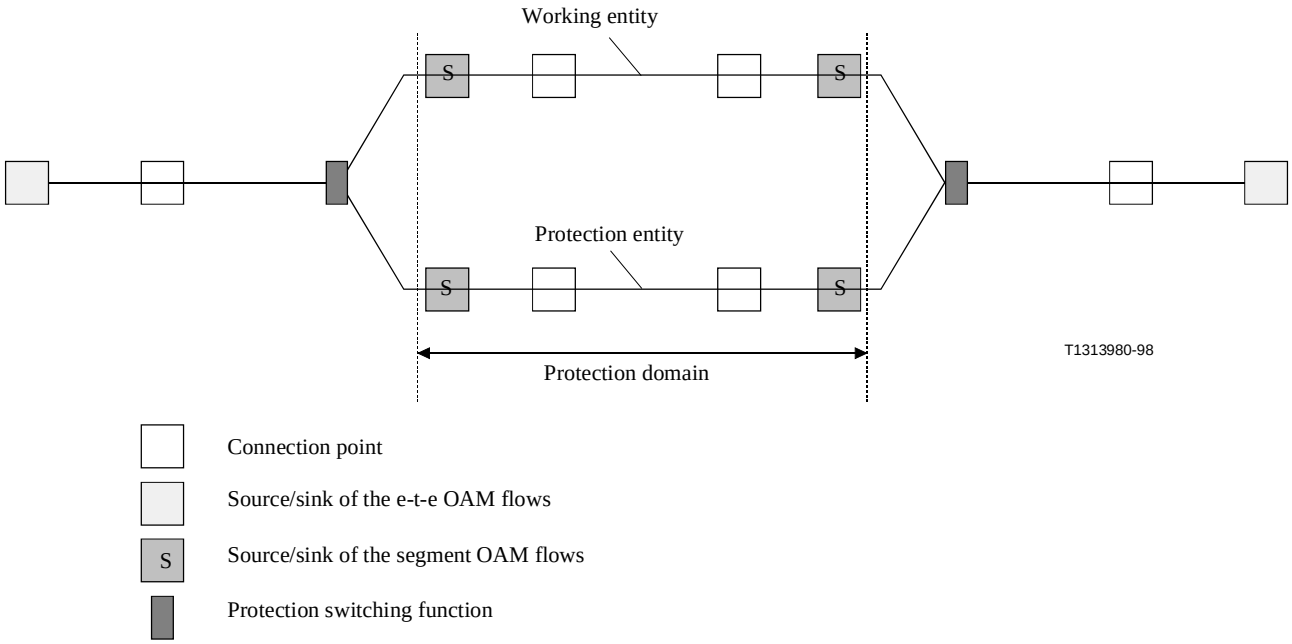


Figure 5/I.630 – 1+1 or 1:1 SNC/S individual VP/VC protection

Figure 6 shows an example of 1:1 or 1+1 SNC/T group protection.

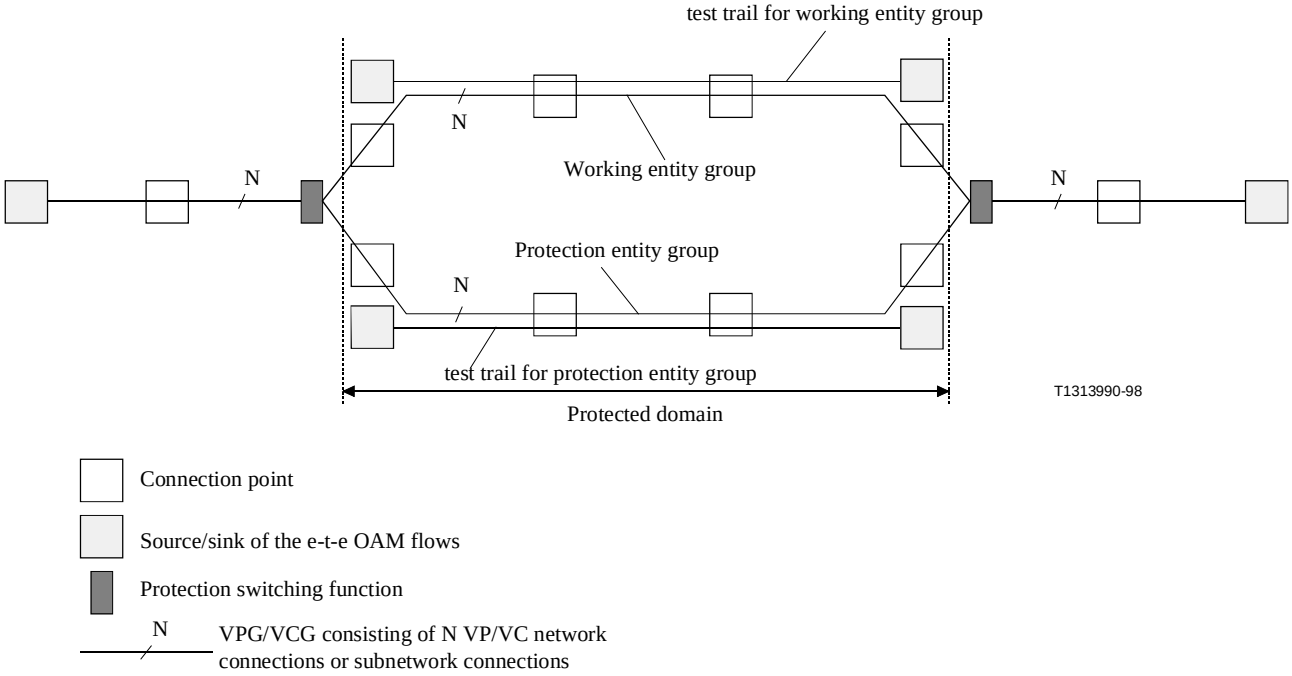


Figure 6/I.630 – 1:1 or 1+1 SNC/T group protection

5.3.3 1+1 non-intrusive monitored subnetwork connection protection (SNC/N)

Figure 7 shows an example of 1+1 non-intrusive monitored individual VP/VC subnetwork connection protection (SNC/N).

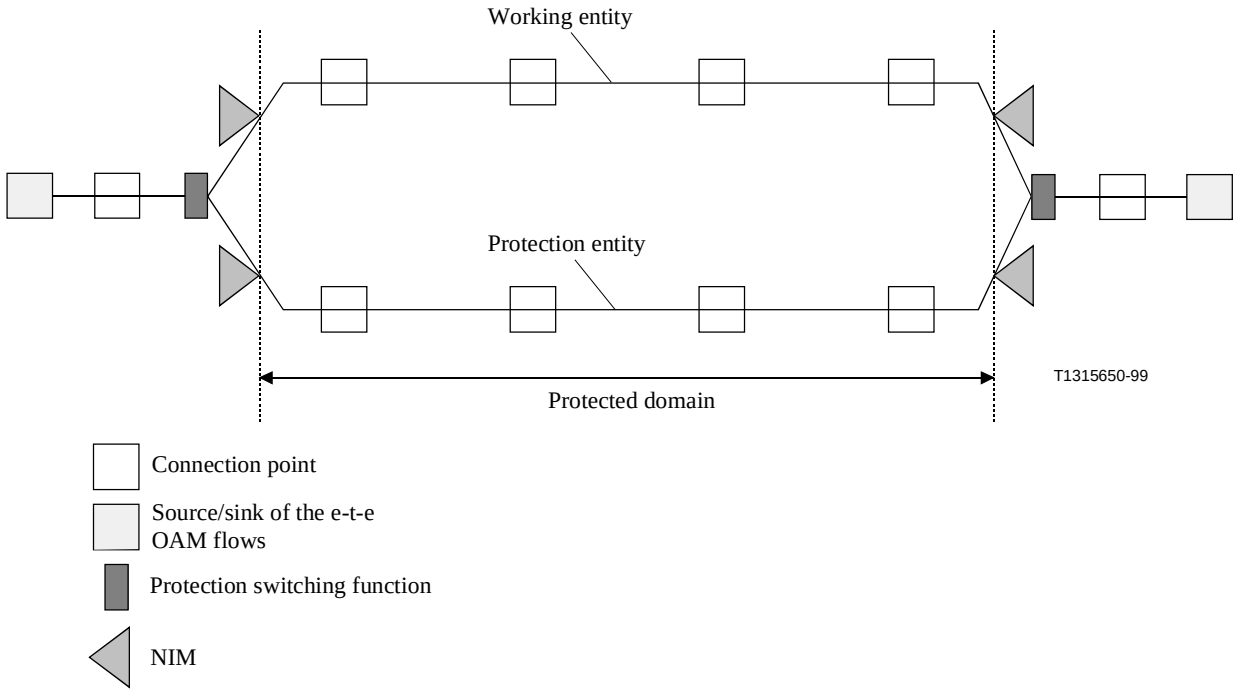


Figure 7/I.630 – 1+1 non-intrusive monitored individual VP/VC SNC/N protection

5.3.4 Relationship between the protected domain and the extent of OAM flows

The configuration where a protected domain and an OAM segment overlaps cannot be supported. The configuration where two protected domains overlap cannot be supported for bidirectional protection switching. Note however that overlapping protected domains can be supported for 1+1 unidirectional protection switching.

5.4 Dependency on physical layer network configuration

Normally, the protection and working entities should be routed on physically diverse transport entities.

5.5 Protection switching configurations

5.5.1 (1:1) configuration

One dedicated protection entity is assigned to each working entity. The protection entity only conveys traffic if the working entity has failed or forced switch/manual switch for working entity operation has been carried out. Otherwise it does not carry traffic and it may carry extra traffic.

5.5.2 (1+1) configuration

One dedicated protection entity is assigned to each working entity. The working and protection entities convey the traffic simultaneously.

5.5.3 (1:n) configuration

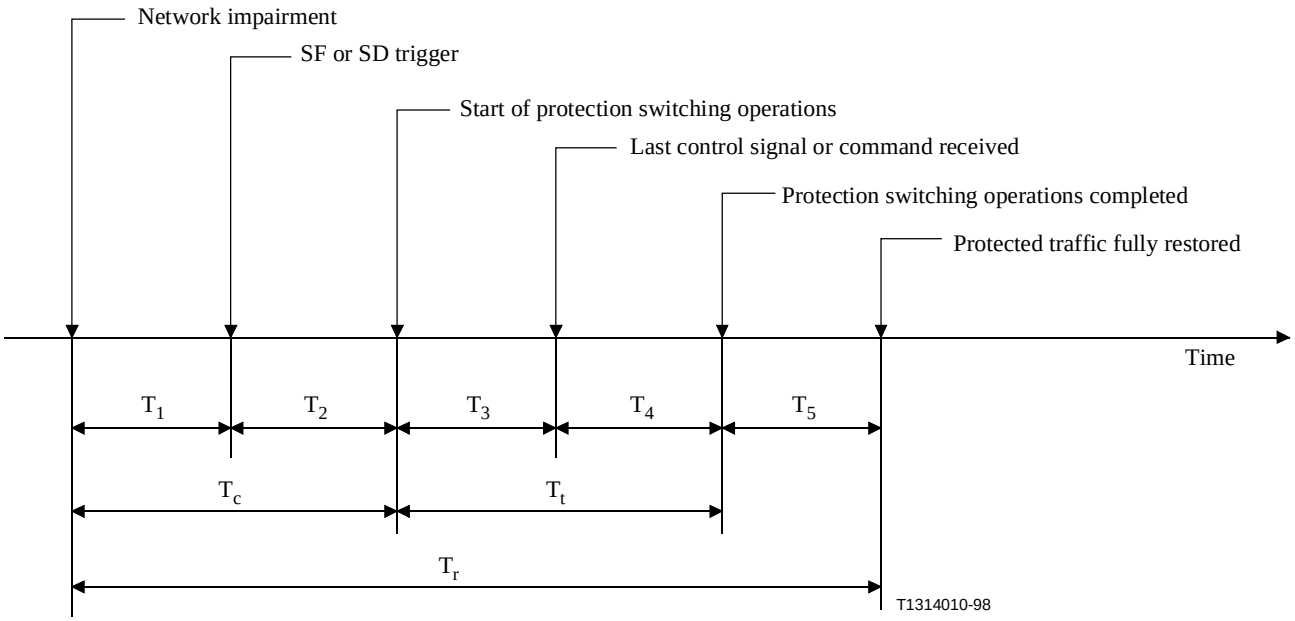
For further study.

5.5.4 (m:n) configuration

For further study.

5.6 Protection switching performance

The ATM protection switching temporal model based on Recommendation M.495 [7] and its parameters are illustrated in Figure 8.



detection time, T_1

waiting time, T_2: [This time corresponds to the hold-off time (see 5.7).]

protection switching operations time, T_3

protection switching transfer time, T_4

recovery time, T_5

confirmation time, T_c

transfer time, T_t

protected traffic restoration time, T_r

Figure 8/I.630 – Protection switching temporal model

5.7 Hold-off function in ATM survivability escalation

In order to give a chance to protect the working traffic to lower layer protection switching functions before ATM layer protection switching takes place, or to confirm the persistency of the defect to protect against, or to delay protection switching for other operational reasons, hold-off time should be provided.

As the VP/VC-AIS cells are transmitted as soon as possible after the detection of a defect, hold-off time is set at the sink of the protected domain. Protection switching operation starts after *x* seconds of an end-to-end or seg_AIS state observed at the sink of the protected domain.

The value of *x* can be selected within the range of 0 to 10 seconds with the granularity of 500 ms.

5.8 Protection switching control protocol

Bidirectional protection switching is realized by exchanging coordination information between source and sink of the protected domain. Coordination information is transmitted using the dedicated VP/VC-APS cell. The format of the VP/VC-APS cell is given in Figure 9. Related code points are

given in Table 1. The detailed description of the protection switching coordination mechanism for (1:1) and (1+1) configurations is provided in Annex A.

(1+1) unidirectional protection switching is realized without a coordination protocol. Details are provided in Annex B.

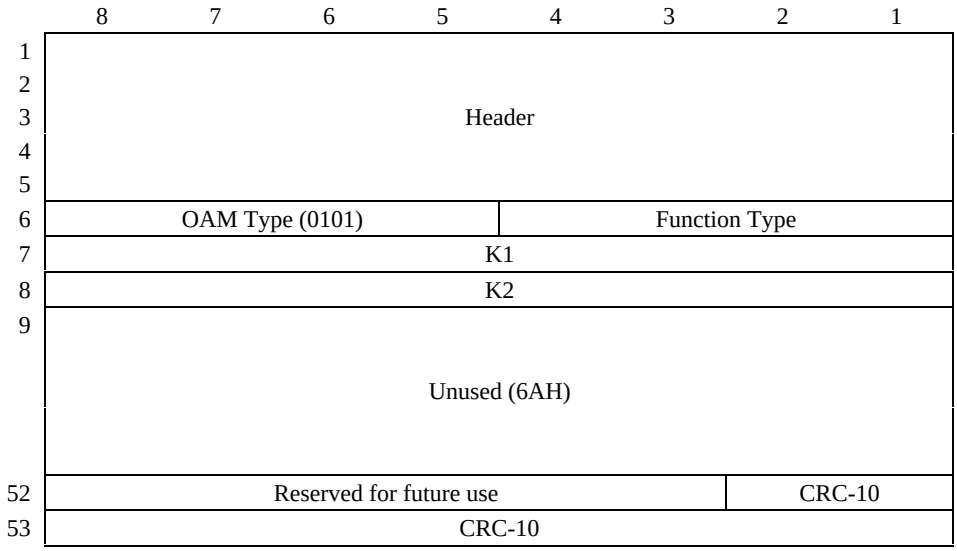


Figure 9/I.630 – APS cell format

Table 1/I.630 – Code points for the APS cell

OAM type	Coding	Function type	Coding
Coordination protocol	0101	Group protection	0000
		Individual protection	0001

6 ATM VP/VC protection switching

6.1 Specific requirements and objectives

General requirements and objectives of 5.1.2 are applicable to ATM VP/VC protection switching.

6.2 Protection switching trigger mechanism

Protection switching should be conducted when:

1) initiated by operator control (e.g. manual switch, forced switch, and lockout of protection);
2) SF is detected;
3) SD is detected; or
4) the "wait to restore" timer expires.

6.2.1 Operator control

Operator control of the protection switching function may be transferred via TMN interfaces (F or Q3 interfaces [8] and [9]).

6.2.2 Trigger for signal fail

For individual VP/VC protection switching (unidirectional or bidirectional) in cases where the protected domain is coupled with an OAM segment, protection switching is initiated when the seg_AIS state continues beyond the provisioned hold-off time at the sink of the protected domain for the working and protection entities respectively.

For individual VP/VC protection switching (unidirectional or bidirectional) in cases where the protected domain is coupled with an end-to-end connection, protection switching is initiated when the e-t-e_AIS state continues beyond the provisioned hold-off time at the sink of the protected domain for the working and protection entities respectively.

For 1+1 individual VP/VC unidirectional protection switching in the case of non-intrusive monitored subnetwork connection protection, protection switching is initiated when the e-t-e_AIS state (determined locally using non-intrusive monitoring) continues beyond the provisioned hold-off time at the sink of the protected domain for the working and protection entities respectively.

The formats of e-t-e_/seg_VP-AIS cell and e-t-e_/seg_VC-AIS cell as well as the declaration and removal conditions of AIS state are specified in Recommendation I.610 [5].

6.2.3 Trigger for signal degrade

Performance degradation of working and protection entities can be detected with the e-t-e or segment performance OAM flows. Details are for further study.

7 ATM VP/VC Group protection switching

7.1 Specific requirements and objectives

General requirements and objectives of 5.1.2 are applicable to ATM VPG/VCG protection switching.

7.2 Architecture

7.2.1 Introduction

The logical entity for protection bundling at the ATM layer is the Virtual Path Group (VPG) and Virtual Channel Group (VCG).

A VPG/VCG (working VPG/VCG [VPG_W/VCG_W] or protection VPG/VCG [VPG_P/VCG_P]) is a logical bundle of one or more ATM VP/VC network and/or subnetwork connections that share the same transmission paths(s) within the protected domain. The VPG/VCG is configured by the operator at the source and also the sink of the protected domain. In the event of protection switching, all the VPs/VCs contained in the VPG/VCG except for the APS VPC/VCC are switched simultaneously. See Figure 10 for an example of VPGs.

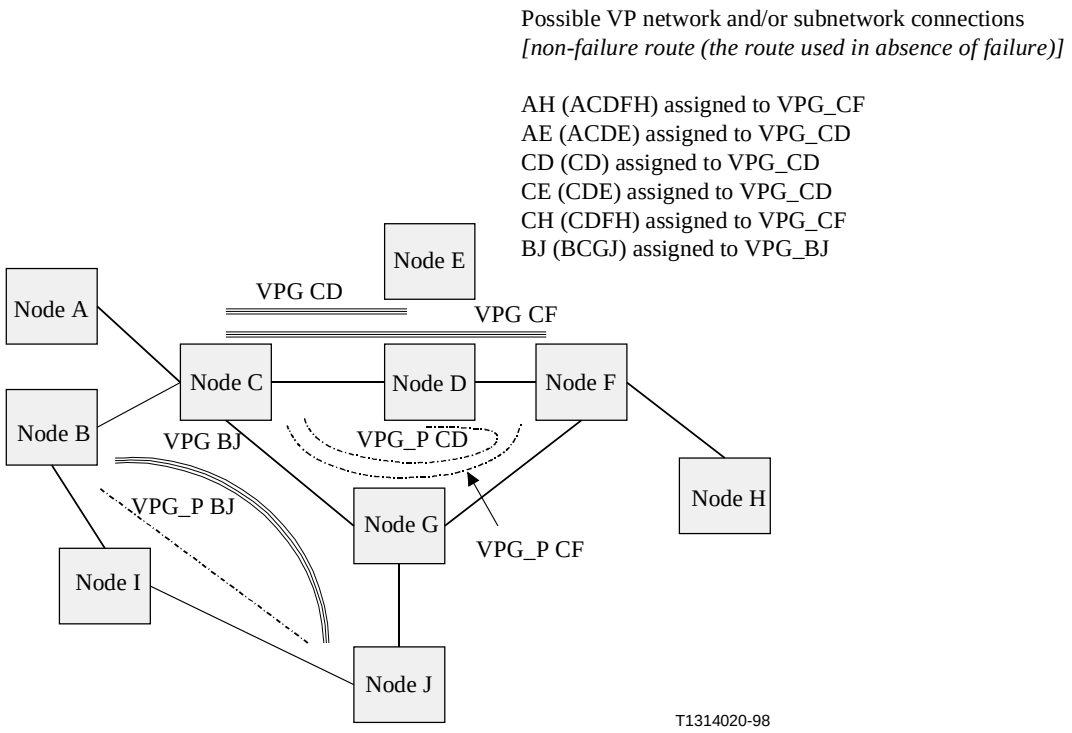


Figure 10/I.630 – An example of VPG

7.2.2 General

The VPG/VCG protection switching scheme defined herein has the following architectural characteristics:

- it utilizes a distributed control algorithm;
- it uses dedicated route and dedicated bandwidth resources for the protection entity;
- the source and sink of the protected domain may either be coupled or decoupled from OAM connection/segment endpoints;
- it is currently defined only for linear configurations and is independent of the server layer topology (i.e. physical layer);
- the initiation of protection action may be delayed for a provisionable period (hold-off time), to allow protection at the server layer(s) to execute first.

7.2.3 VPG/VCG 1+1 protection architecture

Figure 11 illustrates the architecture of the 1+1 VPG/VCG configuration (only one direction of transmission is shown).

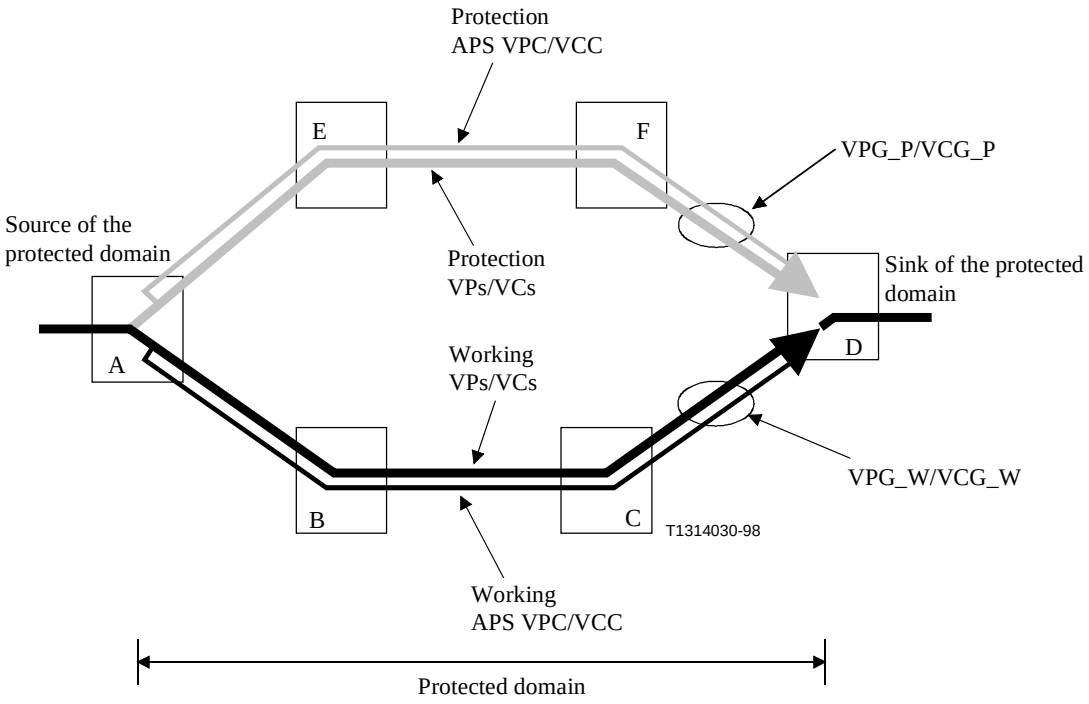


Figure 11/I.630 – 1+1 VPG/VCG configuration

Note that at the source of the protected domain, the working traffic is permanently bridged to the protection entity.

7.2.4 VPG/VCG 1:1 protection architecture

Figure 12 illustrates the architecture of the 1:1 VPG/VCG configuration (only one direction of transmission is shown).

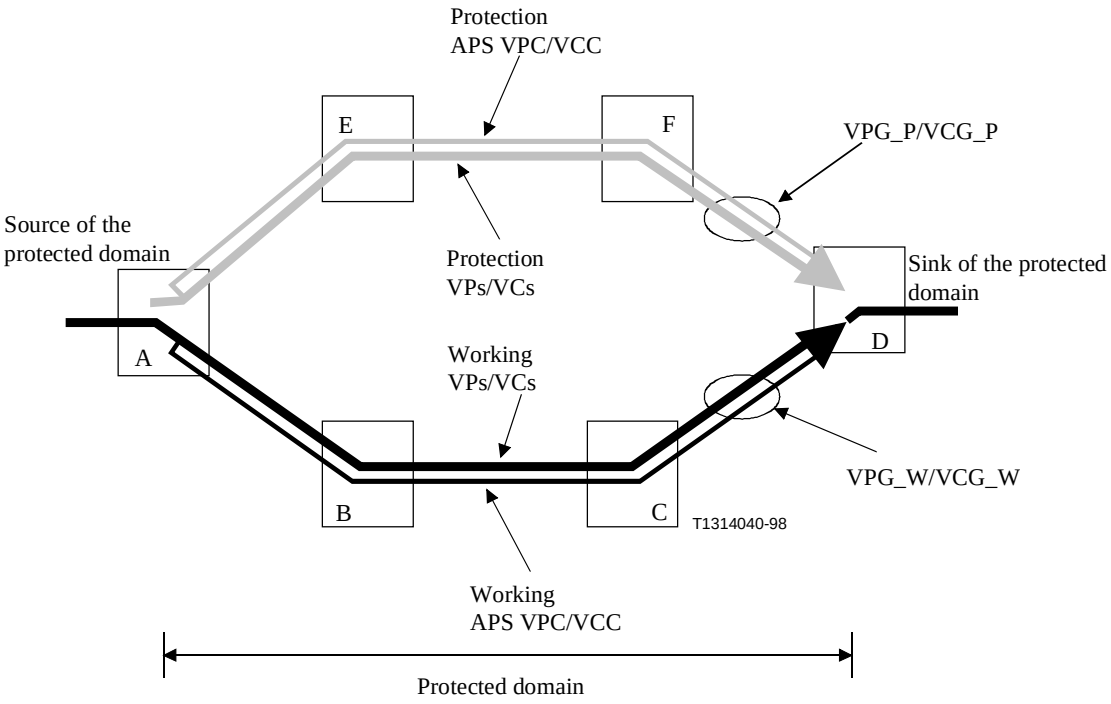


Figure 12/I.630 – 1:1 VPG/VCG configuration

Note that this bridge is viewed functionally as a simple switch (transmitting traffic alternatively to the working or to the protection entities), and not as a broadcast bridge as in Figure 11, where traffic is bridged both to the working and the protection entities.

7.2.5 VPG/VCG 1:N (N>1) protection architecture

For further study.

7.2.6 VPG/VCG M:N protection architecture

For further study.

7.3 Protection switch trigger mechanism

Protection switching should be conducted when:

1) initiated by operator control (e.g. manual switch, force switch, lockout of protection);
2) SF is detected;
3) SD is detected; or
4) the "wait to restore" timer expires.

7.3.1 Operator control

Operator control of the protection switching function may be transferred via TMN interfaces (F or Q3 interfaces [8] and [9]).

7.3.2 Trigger for signal fail

For the group protection (unidirectional or bidirectional) which uses APS VPC/VCC, protection switching is initiated when the end-to-end AIS state continues beyond the provisioned hold-off time at the sink of the protected domain for the associated APS VPC/VCC.

7.3.3 Trigger for signal degrade

For further study.

ANNEX A

Protection switching coordination protocol for 1+1/1:1 configurations

A.1 General introduction

The protection switching coordination protocol described in this annex can be applied to 1+1 and 1:1 linear configurations.

A.1.1 Application architecture

The 1+1/1:1 linear ATM protection switching protocol described in the following subclause may be applied to linear (point-to-point) ATM protection architectures of the protection switching (PS) class, with dedicated protection resource (pre-allocated route and bandwidth) and distributed control (the protection algorithm operates in ATM network elements at both ends of the protection domain).

The protected domain may be an e-t-e VP (or VC) connection, or a segment of a VP (or VC) connection for the individual protection. The application for the case where the protected domain is neither coupled with an e-t-e connection nor coupled with an OAM segment is for further study.

This protocol is also applied to the group protection in addition to the individual protection. APS coordination information is carried through a dedicated connection (APS channel) for the group protection. Protected domain can be aligned with or independent of an e-t-e connection or an OAM segment.

The protocol supports 1+1 architectures. It also supports 1:1 architectures with or without extra traffic. Extra traffic is low priority traffic, which may be transmitted via the protection entity while this is not being used to transmit working traffic.

A 1:1 protection scheme is inherently slower in switching than a 1+1 scheme, requiring communication between both ends of the protection domain to perform even unidirectional switch operation, but it has the advantage of optional support of extra traffic. Also, in 1:1 configurations without extra traffic, the bandwidth of the protection entity is pre-allocated but not in fact used under fault-free conditions.

A.1.1.1 1+1 Architecture

Figure A.1 illustrates the 1+1 linear protection switching architecture. Traffic is permanently bridged to both the working entity (#1) and the protection entity (#0). In this Figure, traffic is shown as being received via the selector from the working entity (#1). Note that the selector function uses VPI/VCI routing functionality and may be implemented in two ways:

– as a change to VPI/VCI routing tables that is made in the case of a protection switch; or

– by simply inhibiting traffic either from the working or the protection entity, with VPI/VCI routing tables configured for a logical "OR" function of all traffic from the working and from the protection entity.

Figure A.2 illustrates a situation where a (bidirectional) protection switch has occurred, due to a signal fail condition on the working entity (#1).

A.1.1.2 1:1 Architecture

Figure A.3 illustrates the 1:1 linear protection switching architecture, with working traffic being transmitted via working entity (#1). The extra traffic which is transmitted on the protection entity is optional. The selector function for working traffic is the same function as for the 1+1 architecture. The selector for extra traffic also uses VPI/VCI routing functionality so traffic is routed according to the VPI/VCI value to the extra traffic output.

Figure A.4 illustrates a situation where a (bidirectional) protection switch has occurred, due to a signal fail condition on the working entity (#1). At the transmit side, working traffic is bridged to the protection entity and extra traffic is dropped. Note that this bridge is viewed functionally as a simple switch (transmitting traffic alternatively to the working or to the protection entities), and not as a broadcast bridge as in Figure A.1, where traffic is bridged both to the working and the protection entities. At the receive side, the selector is activated, so working traffic is received from the protection entity. At the same time, the reception of extra traffic is inhibited and AIS is inserted downstream on the extra traffic output. During protection switching operation, transient mismatch between bridge/selector positions at locations WEST and EAST is possible. However, misconnections between working and extra traffic are not possible, because traffic is always routed correctly through the selector function, based on the VPI/VCI value, either to the working or to the extra traffic output. Note that in order to achieve this VPI/VCI routing, different VPI/VCI values must be configured on the protection entity for working and for extra traffic. This may be automatically achieved by configuring an individual VPI/VCI route for working traffic via the protection entity; traffic is then only bridged to this route in the case of protection switching. Note that in the case of individual VP/VC protection, if different VPI/VCI values are configured on the protection entity for working and for extra traffic, then the supervision of SF/SD and the protection protocol communication only apply to the VPI/VCI value configured for the working traffic.

The routing of traffic according to the VPI/VCI value in the selector function means that for 1:1 architectures traffic misconnections are never possible. This greatly simplifies the functionality of the protection switching protocol, enabling a one-phase protocol to be used, with only a single information exchange being required between both ends to complete a bidirectional switch. In contrast, for multiplex section protection of SDH networks VPI/VCI routing is not possible. Thus a two- or three-phase protection protocol is required in the case of 1:n architectures, in order to avoid situations where a selector might be activated before a bridge, creating temporary misconnections between working and extra traffic.

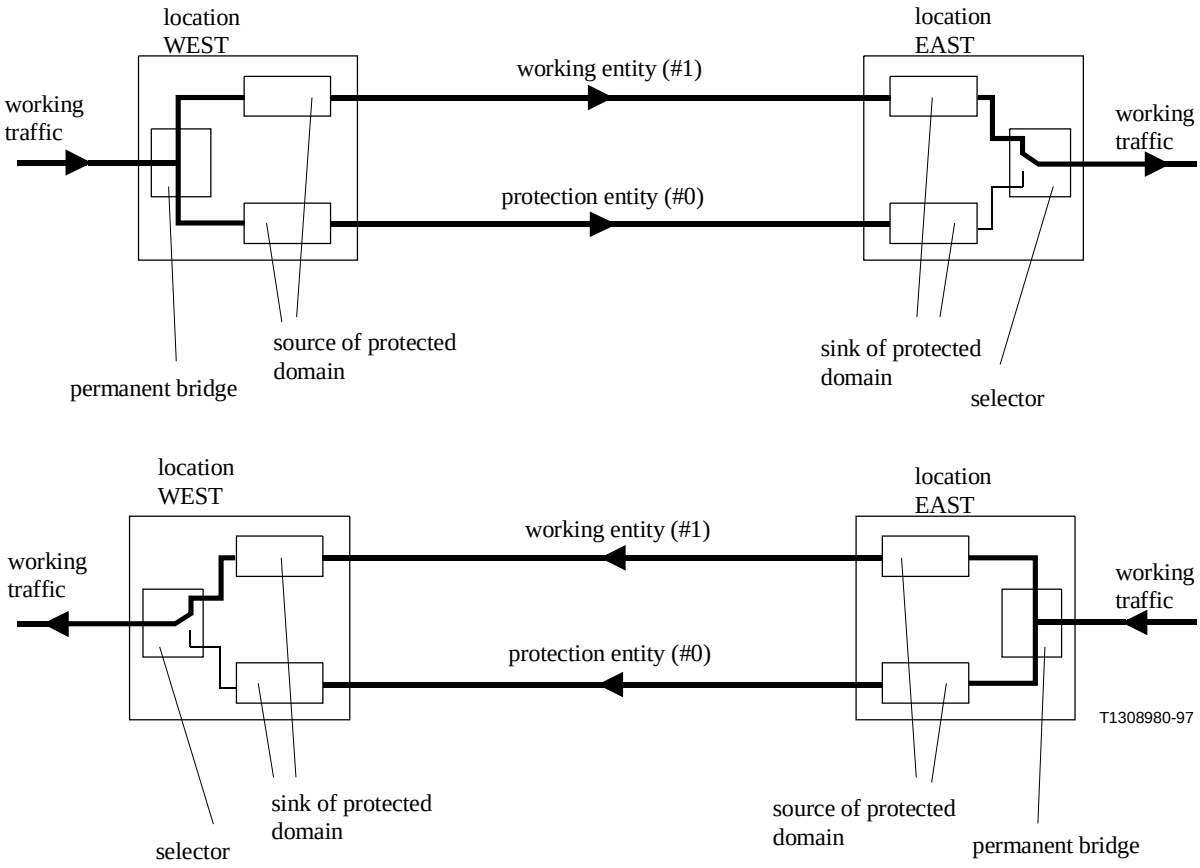


Figure A.1/I.630 – 1+1 Linear protection switching architecture – selector is positioned to receive traffic from working entity (#1)

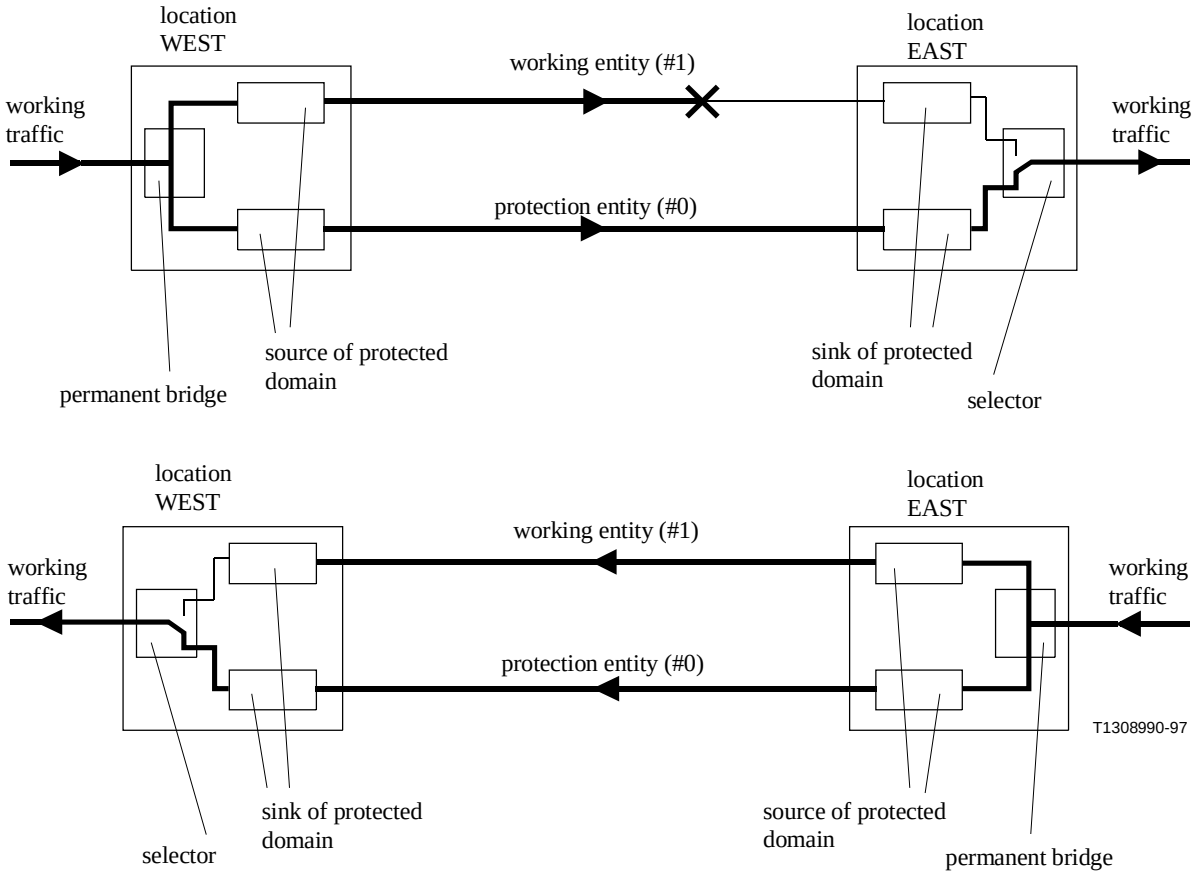


Figure A.2/I.630 – 1+1 Linear protection switching architecture – selector is positioned to receive traffic from protection entity (#0), due to unidirectional signal fail condition for working entity (#1)

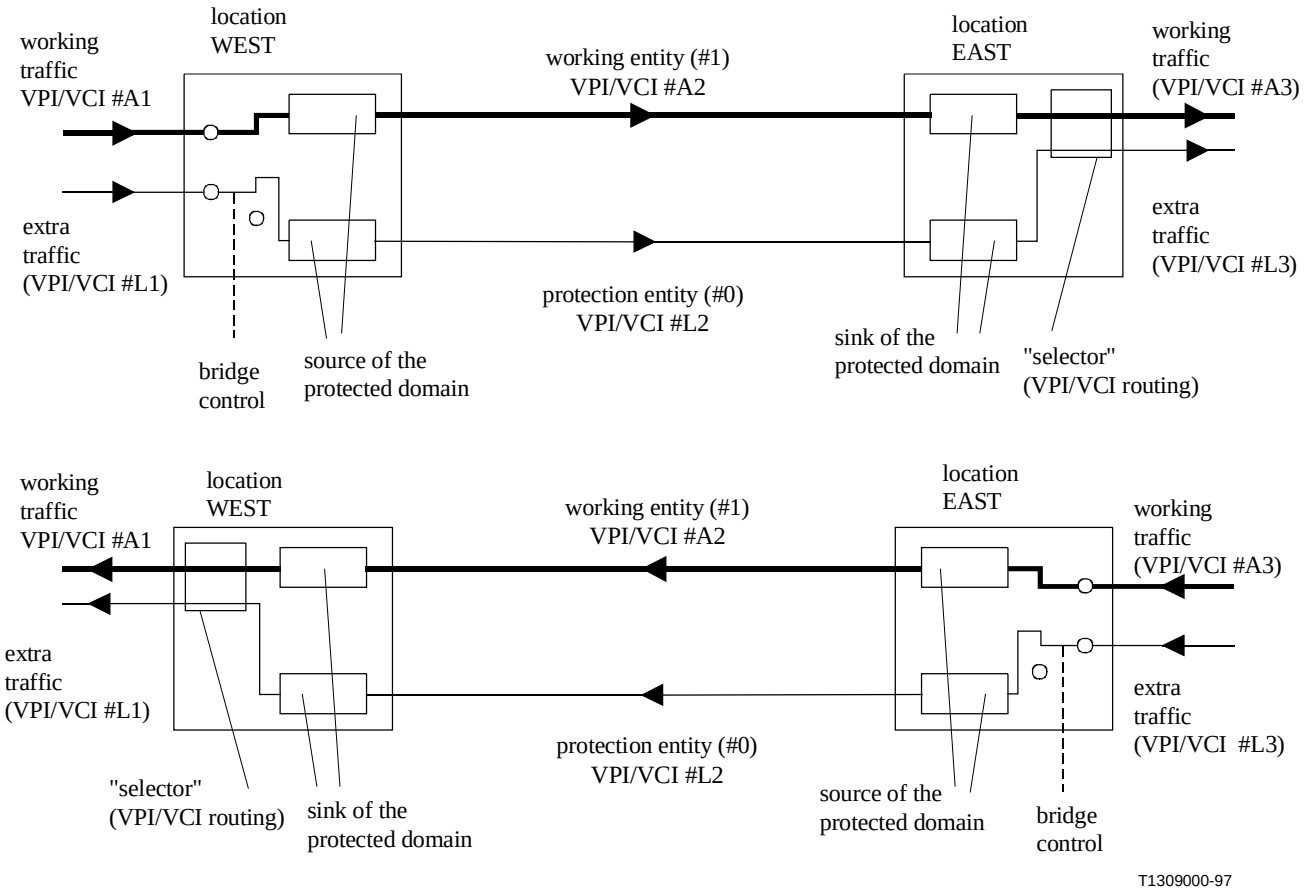


Figure A.3/I.630 – 1:1 Linear protection switching architecture – transmission of working traffic via working entity (#1)

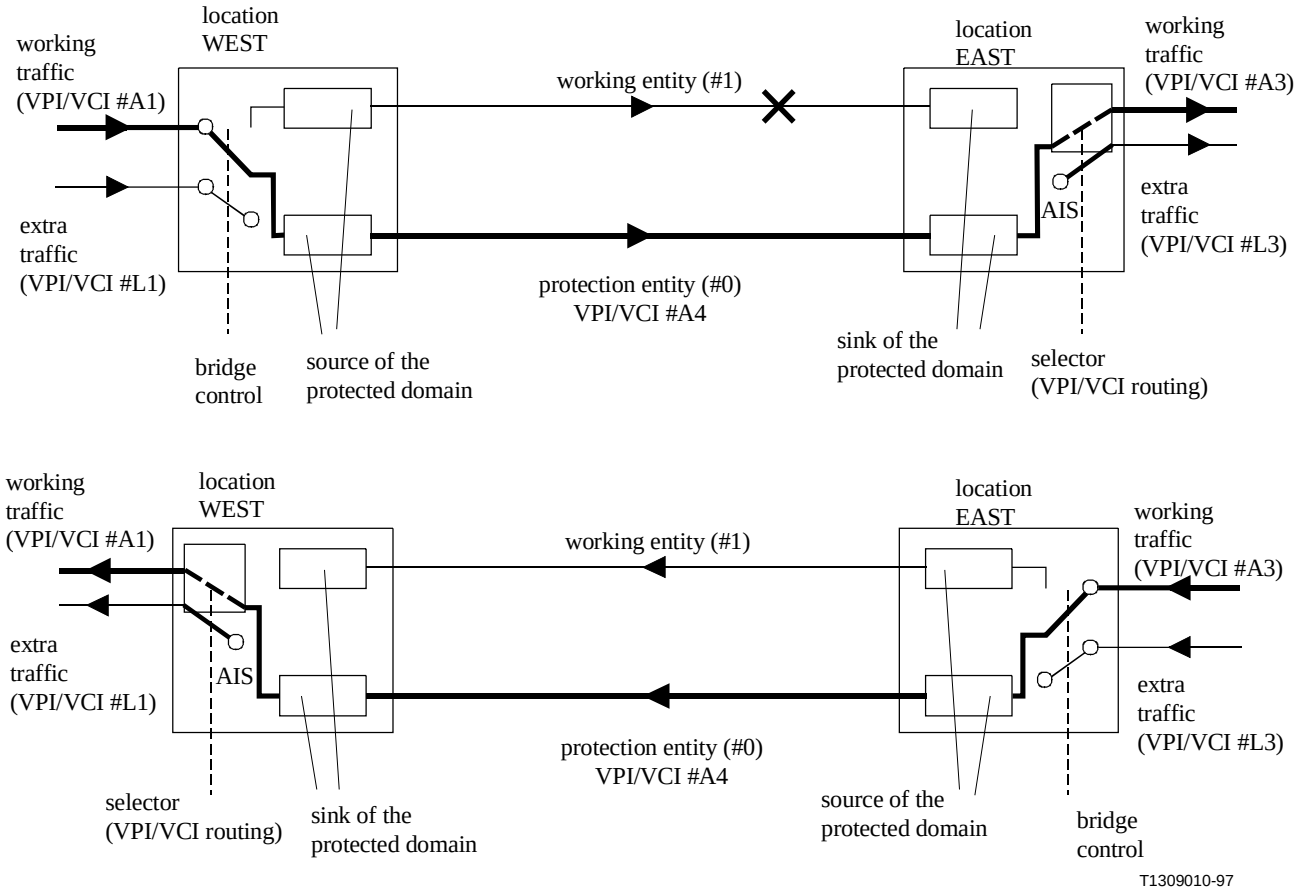


Figure A.4/I.630 – 1:1 Linear protection switching architecture – transmission of working traffic via protection entity (#0) due to unidirectional Signal Fail condition for working entity (#1)

A.1.2 Compliance with network objectives

Important network objectives are discussed with respect to how they are fulfilled by the linear ATM protection switching protocol described in A.2.

1) *Extent of protection*

For a single point failure, all traffic that would be passing through the failed location, had no failure occurred, is restored. In the case of multiple failures, the failure with the highest priority takes precedence. For example, an SF type failure overrides an SD type failure.

2) *Switching types*

Bidirectional switching is supported by this annex.

3) *Protection switching protocol*

The PS protocol is simple, fast and robust. Simplicity facilitates implementation and transparency of operation. A fast (or "handshake optimized") protocol makes it easier for the required switch completion time to be met. The protocol is robust, due to its inherent simplicity, thus making a malfunction (due to residual implementation errors) unlikely.

4) *Operating modes*

Revertive switching is provided. For 1:1 architectures without extra traffic and for 1+1 architectures, non-revertive switching is also possible.

5) *Manual control*

Operator control via freeze local protection switching function, lockout of protection, forced switch and manual switch commands are supported. Exercise commands are not necessary, due to the simplicity of the protocol.

6) *Other switch initiation criteria*

Signal fail, signal degrade, wait to restore, do not revert and no request are supported in addition to the manual control commands listed above, as criteria for initiating (or preventing) a protection switch.

A.2 1+1/1:1 Linear protection switching protocol

A.2.1 Switch initiation criteria

The following switch initiation criteria exist:

1) an externally initiated command (clear, freeze local protection switching function, lockout of protection, forced switch, manual switch);

2) an automatically initiated command (signal fail or signal degrade) associated with a protection domain; or

3) a state (wait to restore, do not revert, no request) of the protection switching function.

A.2.1.1 Externally initiated commands

Externally initiated commands are listed below in descending order of priority. Each command may be applied either to the WEST or to the EAST network element of a linear APS scheme (see e.g. Figure A.1.

Clear: Clears all switch commands listed below for the associated network element. Note that the Clear command is only used to reset freeze local protection switching function, lockout of protection, forced switch or manual switch command. This command is not signalled via the protection switching protocol.

Freeze local protection switching function: This command freezes (maintains) the current bridge/selector position and the currently transmitted K1/K2 byte values for the local protection switching function. It has the highest priority of all externally initiated commands other than clear. Thus, local requests other than clear are ignored when this command is in effect. Note that the K1/K2 bytes received from the far end continue to be evaluated so that local detection of bridge/selector mismatch remains possible. This command is not signalled via the protection switching protocol.

NOTE – This command is mainly intended for maintenance purpose. When maintenance work is conducted on the working entity, it may be requested that the working entity is not used even if the protection entity fails. For this purpose, FS command cannot be used because FS command would be overridden by SF for protection entity. An example of a possible maintenance scenario for this purpose is:

1) Confirm that the protection entity is not failed.

2) Issue an FS command to switch to the protection entity.

3) Issue an "freeze local protection switching function" command.

4) Conduct maintenance work on the working entity.

5) Clear the "freeze local protection switching function" command.

Lockout of protection (LoP): Denies all working traffic (but not extra traffic) access to the protection entity.

Forced Switch (FS) for working entity (#1): Bridges/switches working traffic (#1) to the protection entity, unless a Signal Fail condition exists for the protection entity. Note that Forced Switch for protection entity (#0) is not defined, as this functionality is accomplished by a Lockout of protection command.

Manual Switch (MS) for protection entity (#0): Denies working traffic access to the protection entity unless a higher priority request (such as SF or SD for a working entity) is in effect.

Manual Switch (MS) for working entity (#1): Bridges/switches working traffic (#1) to the protection entity, unless a higher priority request is in effect.

Note that exercise commands, as defined for some more complex protection protocols, are not required and therefore not defined.

A.2.1.2 Automatically initiated commands

To prevent frequent transitions, the transition of signal fail from the active to the inactive condition shall only occur if the AIS state remains continuously cleared for a persistency time of 5 seconds.

A.2.1.3 States

Wait to Restore (WTR) is only applicable for revertive mode and applies to a working entity (#1). This state is entered by the local protection switching function in conditions where working traffic (#1) is being received via the protection entity, if local protection switching requests (see Figure A.5) have been previously active and now become inactive. It prevents reversion back to the released bridge/selector position until the wait to restore time has expired. The wait to restore time may be configured by the operator in 1 minute steps between 1 and 30 minutes; the default value is 12 minutes.

Do Not Revert (DNR) is only applicable for non-revertive mode (which is possible in 1:1 architectures without extra traffic or in 1+1 architectures) and is only defined for working entity (#1). This state is entered by the local protection switching function in conditions where working traffic (#1) is being transmitted via the protection entity, if local protection switching requests (see Figure A.5) have been previously active and now become inactive. It prevents reversion back to the released bridge/selector position in non-revertive mode under no request conditions.

No Request [(NR); which is only defined for the protection entity (#0)] is the state entered by the local protection switching function (see Figure A.5) under all conditions where no local protection switching requests (including wait to restore and do not revert) are active; note that this may occur when the bridge/selector is activated or when it is released.

A.2.2 K1/K2 byte generation rules

NOTE – Bit 1 is the most significant bit (MSB) and bit 8 is the least significant bit (LSB) in this annex.

For linear 1+1/1:1 protocol operation, protocol information is conveyed between the network elements at locations WEST and EAST via 2 bytes of information called K1 and K2 bytes. These 2 bytes are transported by APS cells via the protection entity (see for example Figure A.1), being inserted by the protection domain source function and extracted by the protection domain sink function. For the K1 byte all 8 bits are defined; for the K2 byte only the first 4 bits are defined.

The bit assignments for linear 1+1/1:1 protocol operation are defined as follows:

Bits 1-8 of the K1 byte indicate a request for switch action of the protection switching local priority logic (see Figure A.5).

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

Bits 5-8 of K1 indicate the associated entity number, i.e. whether the request applies to the working entity (#1 to #n, with n being less than or equal to 15) or to the protection entity (#0), as follows:

Bits 5678	
0000	if the request applies to the protection entity.
0001	if the request applies to the working entity (#1).

Bits 1-4 of the K2 half-byte indicate the local bridge/selector status of the protection switching global priority logic (see Figure A.5), as follows:

For 1+1 operating mode, the selector position of the local network element is indicated, i.e.:

Bits 1234	
0000	if the selector is activated to receive traffic from the protection entity (see Figure A.2).
0001	if the selector is released to receive traffic from the working entity (#1) (see Figure A.1).

For 1:1 operating mode, the bridge/selector position of the local network element is indicated, i.e.:

Bits 1234	
0000	if the bridge/selector is released so all working traffic is transmitted via the associated working entities and extra traffic (if configured) is transmitted via the protection entity.
0001	if the bridge/selector is activated to transmit working traffic (#1) via the protection entity.

Note that the different strategy for coding the K2 byte for 1+1 and for 1:1 operation ensures that a mismatch alarm will be automatically generated if the network element at one end of the protection domain is configured for 1+1 operation and the other end is (unintentionally) configured for 1:1 operation.

Bits 5-8 of the K2 byte are not used for linear 1+1/1:1 protocol operation.

Table A.1/I.630 – K1 byte coding of requests

K1 Byte Coding: Bits 1234	Request (i.e. automatically initiated command, state, or externally initiated command)	Order of Priority
1111	Lockout of protection (Note 1)	Highest
1110	Signal fail for protection entity (Note 1)	|
1101	Forced switch for working entity (#1) (Note 5)	|
1100	Reserved for future use (Note 2)	|
1011	Signal fail for working entity (#1)	|
1010	Reserved for future use (Note 2)	|
1001	Signal degrade for protection entity	|
1000	Signal degrade for working entity (#1)	|
0111	Reserved for future use (Note 2)	|
0110	Manual switch for protection entity	|
0101	Manual switch for working entity (#1)	|
0100	Reserved for future use (Note 2)	|
0011	Wait to restore for working entity (#1) (Note 3)	|
0010	Reserved for future use (Note 2)	|
0001	Do not revert for working entity (#1) (Note 4)	|
0000	No request (Note 1)	Lowest

Note that in the case that more than one request of the same priority listed in this Table 1 is simultaneously active, the request with the lowest entity number takes precedence. Therefore, a request (e.g. Signal Degrade) for the protection entity (#0) overrides the same request for the working entity (#1).

NOTE 1 – Only K1 bits 5-8 coding of "0000" is allowed with No Request, Lockout of protection, signal fail for protection entity, signal degrade for protection entity, and manual switch for protection entity.

NOTE 2 – These codes are ignored by the receiver.

NOTE 3 – Wait to restore for working entity (#1) is only applicable for revertive operation.

NOTE 4 – Do not revert for working entity (#1) is only applicable for non-revertive operation; only K1 bits 5-8 coding of "0001" is allowed.

NOTE 5 – Forced switch for protection entity (#0) is not defined because this function may be achieved via a lockout of protection command.

A.2.3 1+1/1:1 Linear protection switching algorithm

A.2.3.1 Principle of operation

Figure A.5 illustrates the principle of the 1+1/1:1 linear protection switching algorithm. This algorithm is performed in network elements at both ends of the protection domain (locations WEST and EAST). Bidirectional switching is achieved by transmitting local switching requests to the Far End via the K1 byte. The transmitted K2 byte contains the local bridge/selector status information; a persistent mismatch between both ends may thus be detected and leads to an alarm.

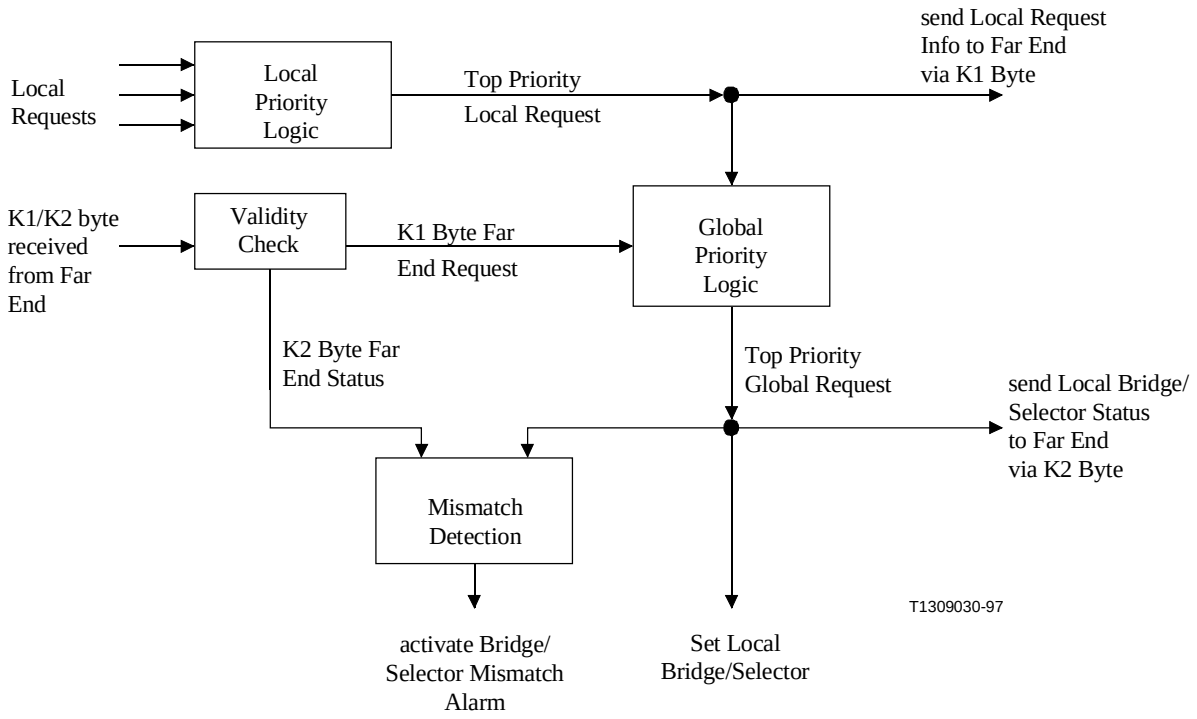


Figure A.5/I.630 – Principle of 1+1/1:1 Linear protection switching algorithm

In detail, the functionality is as follows (see Figure A.5):

At the local network element, one or more local protection switching requests (as listed in A.2.1) may be active. The "local priority logic" determines which of these requests is of top priority, using the order of priority given in Table A.1. This top priority local request information is transmitted to the far end via the K1 byte (with coding as described in A.2.2). It is also passed on to the "global priority logic".

The local network element receives information from the network element of the far end via the K1 and K2 bytes. The received K1/K2 bytes are subjected to a validity check (see A.2.3.4). The information of the received K1 byte (which indicates the top priority local request of the far end) is then passed to the "global priority logic". The "global priority logic" compares the top priority local request with the request of the received K1 byte (according to the order of priority of Table A.1) to determine the top priority global request. This request then determines the bridge/selector position (or status) of the local network element as follows:

– for 1+1 architectures (see Figures A.1 and A.2), only the selector position is controlled. For 1:1 architectures (see Figures A.3 to A.5), both the bridge and the selector positions are controlled simultaneously, i.e. whenever the bridge of a network element is activated (or released), the selector of the same network element is activated (or released) at the same time;
– if the top priority global request is a request for a working entity (see Table A.1), the associated working traffic is bridged/switched to/from the protection entity, i.e. the associated bridge/selector of the local network element is activated;
– if the top priority global request is a request for the protection entity (see Table A.1), no working traffic is bridged/switched to/from the protection entity, i.e. the associated bridge/selector of the local network element is released.

The bridge/selector status is transmitted to the far end via the K2 byte (with coding as described in A.2.2). It is also compared with the bridge/selector status of the far end as indicated by the received

K2 byte: if a mismatch between the positions of the near end and the far end persists for more than *m* seconds, the bridge/selector mismatch alarm is raised for the local network element. The persistency time *m* seconds should be long enough to allow for 3 lost APS protocol cells before generating the alarm.

Note that the linear protection switching algorithm commences immediately every time one of the input signals (see Figure A.5) changes, i.e. when the status of any local request changes, or when a different K1/K2 byte is received from the far end. The consequent actions of the algorithm are also initiated immediately, i.e. change the local bridge/selector position (if necessary), transmit a new K1/K2 byte status (if necessary), or activate the Bridge/Selector Mismatch Alarm (if the persistency time has expired).

A.2.3.2 Revertive mode

In revertive mode of operation, in conditions where working traffic (#1) is being received via the protection entity, if local protection switching requests (see Figure A.5) have been previously active and now become inactive, a local wait to restore state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted K1 byte and maintains the switch.

This state normally times out and becomes a no request state after the wait to restore timer (see A.2.1.3) has expired. The wait to restore timer deactivates earlier if any local request of higher priority pre-empts this state.

Note that for the decision of whether or not to enter the wait to restore state, only local requests are considered. A switch to the protection entity may be maintained by a local wait to restore state or by a remote request (wait to restore or other) received via the K1 byte. Therefore, in a case where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both wait to restore timers at both ends have expired.

A.2.3.3 Non-revertive mode

Non-revertive mode is only applicable (as an option to revertive mode) for 1+1 architectures or for 1:1 architectures in configurations without extra traffic.

In non-revertive mode of operation, in conditions where working traffic (#1) is being transmitted via the protection entity, if local protection switching requests (see Figure A.5) have been previously active and now become inactive, a local do not revert state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted K1 byte and maintains the switch, thus preventing reversion back to the released bridge/selector position in non-revertive mode under no request conditions.

A.2.3.4 Transmission and acceptance of protection protocol bytes

The bytes K1/K2 of the protection protocol are transported by APS cells via the protection entity (see for example Figure A.1), being inserted by the protection domain source function and extracted by the protection domain sink function.

A new APS cell must be transmitted immediately when a change in the transmitted K1 or K2 byte status (see Figure A.5) occurs.

To prevent flooding of APS cells in cases where the sensor for signal fail oscillates rapidly, during processing of local requests (see Figure A.5) the transition of signal fail from the active to the inactive condition shall only occur if the AIS state remains continuously cleared for a persistency time of 5 seconds.

To ensure protocol operation in situations where APS cells are lost or invalid, an APS cell with the current K1/K2 byte transmit status will be transmitted by the network element in steady-state conditions every 5 seconds ("keep alive" mechanism). This eliminates the need for complex retransmit protocol scenarios in case of lost or invalid APS cells. For 1:1 architectures, this will lead to delayed protection switch completion by 5 seconds in the case that an APS cell is lost or invalid.

If no valid K1/K2 bytes are received, the last valid received bytes remain applicable. During signal fail conditions of the protection entity (extended by 5 seconds as described previously), K1/K2 bytes are not evaluated.

A.2.3.5 Protocol example for 1+1 architecture in non-revertive mode

Table A.2 illustrates protection switching action (in non-revertive mode) for this scheme.

When traffic is being received from the working entity (#1) under no failure conditions, No request with entity number "0" is indicated for the transmitted K1 bytes at both ends. Bits 1-4 of the K2 bytes transmitted at both ends are set to "0001" to indicate that the selector is released and receiving traffic from the working entity (#1). See Figure A.1 for an illustration.

The global priority logic of each end determines the top priority global request that is active. This may be a far end request (received via the K1 byte) or a local request. The global priority logic will set the local selector in accordance with the top priority global request. The resultant selector position will be indicated in K2 bits 1-4. For the generation of the transmitted K1 byte, only the top priority local request is considered; far end requests are never considered.

In the example, SF is detected at the EAST location on the working entity (#1). Consequently, the global priority logic at EAST will activate the selector to receive traffic from the protection entity (#0). The global priority logic at WEST detects the failure via the received K1 byte and also activates its selector, maintaining "no request" for the transmitted K1 byte, as no local request is active. See Figure A.2 for an illustration.

After repair of the working entity (#1), "do not revert" is indicated at EAST and the selectors at EAST and WEST remain activated. The system does not revert back to a preferred entity as in the case of revertive operation. Note that "do not revert" is removed if pre-empted by a local request. Therefore, if a SD type failure of the protection entity (#0) is subsequently detected at EAST, this will be indicated in the transmitted K1 byte at EAST and the selector at EAST will be released. The global priority logic at WEST detects the failure via the received K1 byte and also releases its selector.

After the protection entity (#0) has been repaired, "No Request" is once again indicated at both ends.

Note that for the same example with operation in revertive mode, "do not revert" will never be indicated. After repair of the working entity (#1), "wait to restore" is indicated at EAST instead of "do not revert". Note that "wait to restore" is removed and the timer reset if pre-empted by a local request. When the wait to restore timer expires, both selectors are released to receive traffic from the working entity (#1) and "No Request" is indicated at both ends.

Table A.2/I.630 – Protocol example for 1+1 architecture in non-revertive operating mode

Failure condition	Coding of protocol bytes				Action	
	EAST → WEST		WEST → EAST			
Bits	Byte K1 12345678	Byte K2 1234	Byte K1 12345678	Byte K2 1234	At EAST	At WEST
No failures. Traffic is received from working entity (#1)	00000000	0001	00000000	0001	Selector is released	Selector is released
Working entity (#1) failed in direction WEST → EAST	10110001	0000	00000000	0001	Detect local request. Activate selector; update K1/K2.	
	10110001	0000	00000000	0000		Detect Far End request. Activate selector; update K1/K2.
Working entity (#1) repaired	00010001	0000	00000000	0000	Detect local request clear; enter do not revert state; update K1.	
Protection entity (#0) degraded in direction WEST → EAST	10010000	0001	00000000	0000	Detect local request. Release selector; update K1/K2.	
	10010000	0001	00000000	0001		Detect Far End request. Release selector; update K1/K2.
Protection entity (#0) repaired	00000000	0001	00000000	0001	No Request state. Update K1.	

A.2.3.6 Protocol example for 1:1 architecture in revertive mode

Table A.3 illustrates protection switching action (in revertive mode) for this scheme.

During normal working conditions, all working traffic is transmitted via the associated working entities and extra traffic (if configured) is transmitted via the protection entity (#0). The bridges/switches at WEST and EAST are released. "No Request" with entity number "0" is indicated for the transmitted K1 bytes at both ends, and "0000" for the transmitted K2 bytes at both ends.

The global priority logic of each end determines the top priority global request that is active. This may be a Far End request (received via the K1 byte) or a local request. The global priority logic will set the local bridge/selector in accordance with the top priority global request. The resultant

bridge/selector position will be indicated in K2 bits 1-4. For the generation of the transmitted K1 byte, only the top priority local request is considered; Far End requests are never considered.

In the example, SF is detected at the EAST location on the working entity (#1). Consequently, the global priority logic at EAST will activate the bridge/selector to transmit working traffic (#1) to the protection entity (#0). The global priority logic at WEST detects the failure via the received K1 byte and also activates its bridge/selector, maintaining "No Request" for the transmitted K1 byte, as no local request is active. See Figure A.5 for an illustration.

After repair of the working entity (#1), "wait to restore" is indicated at EAST and the bridges/switches at EAST and WEST remain activated. Note that "wait to restore" would be removed and the timer reset if pre-empted by a local request. When the wait to restore timer at EAST expires, the No Request state is entered at EAST, the bridge/selector is released and the transmitted K1/K2 bytes are updated. Thus normal working in the failure-free state once again resumes.

Table A.3/I.630 – Protocol example for 1:1 architecture in revertive operating mode

Failure condition	**Coding of protocol bytes**				**Action**	
	EAST → WEST		**WEST → EAST**			
Bits	**Byte K1 12345678**	**Byte K2 1234**	**Byte K1 12345678**	**Byte K2 1234**	**At EAST**	**At WEST**
No failures. All working traffic transmitted via associated working entities	00000000	0000	00000000	0000	Bridge/selector is released	Bridge/selector is released
Working entity (#1) failed in direction WEST → EAST	10110001	0001	00000000	0000	Detect local request. Activate bridge/selector for working traffic (#1); update K1/K2.	
	10110001	0001	00000000	0001		Detect Far End request. Activate bridge/selector for working traffic (#1); update K2.
Working entity (#1) repaired	00110001	0001	00000000	0001	Detect local request clear. Enter wait to restore state for working traffic (#1); update K1.	

Table A.3/I.630 – Protocol example for 1:1 architecture in revertive operating mode *(concluded)*

Failure condition	Coding of protocol bytes				Action	
	EAST → WEST		WEST → EAST			
Bits	Byte K1 12345678	Byte K2 1234	Byte K1 12345678	Byte K2 1234	At EAST	At WEST
Wait to Restore expired at EAST	00000000	0000	00000000	0001	No Request state. Release bridge/selector; update K1/K2.	
	00000000	0000	00000000	0000		No Requests (local or from Far End). Release bridge/selector; update K2.

ANNEX B

1+1 unidirectional SNC and trail protection switching operation

B.1 Application architecture

The 1+1 linear protection switching architecture is as shown in Figure A.1. In the case of unidirectional protection switching operation as described in Annex B, a protection switch is performed by the selector at the protection domain sink based on purely local information.

For example, if a unidirectional failure (in the direction of transmission WEST to EAST) occurs for the working entity in Figure A.1, this failure will be detected at the protection domain sink at location EAST and the selector at location EAST will switch to the protection entity. Note that the selector at location WEST remains unchanged.

B.2 Compliance with network objectives

The following network objectives apply:

1) *Switching types*

   1+1 unidirectional protection switching is supported by this annex.

2) *Protection switching protocol*

   There is no APS protocol for 1+1 unidirectional SNC and trail protection.

3) *Operating modes*

   Revertive and non-revertive switching are provided.

4) *Manual control*

   Operator control via Lockout of Protection, Forced Switch and Manual Switch commands is supported.

5) *Other switch initiation criteria*

Signal Fail, Signal Degrade, Wait to Restore, and No Request are supported in addition to the manual control commands listed above, as criteria for initiating (or preventing) a protection switch.

B.3 Switch initiation criteria

The following switch initiation criteria exist:

1) an externally initiated command (Clear, Lockout of Protection, Forced Switch, Manual Switch);

2) an automatically initiated command (Signal Fail or Signal Degrade) associated with a protected domain; or

3) a state (Wait to Restore, No Request) of the protection switching function.

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

Table B.1/I.630 – Priority of local requests

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

NOTE 1 – A forced switch for working entity should not be overridden by a Signal Fail on the protection entity. Since unidirectional protection switching is being performed and no APS protocol is supported over the protection entity, Signal Fail on the protection entity does not interfere with the ability to perform a forced switch for working entity.

NOTE 2 – A forced switch for protection entity is not defined because this function may be achieved via a lockout of protection command.

B.3.1 Externally initiated commands

Externally initiated commands are listed below in descending order of priority. The functionality of each is described below.

clear: This command clears all of the externally initiated switch commands listed below.

Lockout of Protection (LoP): Prevents the selector from switching to the protection entity, or switches the selector from the protection to the working entity.

Forced Switch (FS) for working entity: Switches the selector from the working entity to the protection entity (unless a higher priority switch request is in effect).

Manual Switch (MS) for working entity: Switches the selector from the working entity to the protection entity (unless an equal or higher priority switch request is in effect).

Manual Switch (MS) for protection entity: Switches the selector from the protection entity to the working entity (unless an equal or higher priority switch request is in effect).

B.3.2 Automatically initiated commands

To prevent frequent transitions, the transition of Signal Fail from the active to the inactive condition shall only occur if the AIS state remains continuously cleared for a persistency time of 5 seconds.

B.3.3 States

Wait to Restore is only applicable for revertive mode and applies to a working entity. This state is entered by the local protection switching function in conditions where working traffic is being received via the protection entity, if local protection switching requests have been previously active and now become inactive. It prevents reversion back to the released selector position until the Wait to Restore time has expired. The Wait to Restore time may be configured by the operator in 1 minute steps between 1 and 30 minutes; the default value is 12 minutes.

No Request is the state entered by the local protection switching function under all conditions where no local protection switching requests (including Wait to Restore) are active; note that this may occur when the selector is activated or when it is released.

B.4 Protection switching protocol

In the unidirectional 1+1 architecture, there is no APS protocol.

B.5 1+1 unidirectional protection switching algorithm operation

B.5.1 Control of the bridge

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

B.5.2 Control of the selector

In the 1+1 architecture in unidirectional protection switching operation, the selector is controlled by the highest priority local request (automatically initiated command, state, or externally initiated command). Therefore, each end operates independently of the other. If a condition of equal priority (e.g. SF, SD) exists on both entities, switching shall not be performed.

B.5.3 Revertive mode

In revertive mode of operation, under conditions where working traffic is being received via the protection entity, if local protection switching requests have been previously active and now become inactive, a local Wait to Restore state is entered.

This state normally times out and becomes a No Request state after the Wait to Restore timer has expired. The Wait to Restore timer deactivates earlier if any local request of higher priority pre-empts this state.

B.5.4 Non-revertive mode

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

ITU-T RECOMMENDATIONS SERIES

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