International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.8131/Y.1382

(02/2007)

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

Packet over Transport aspects – MPLS over Transport aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

Linear protection switching for transport MPLS (T-MPLS) networks

ITU-T Recommendation G.8131/Y.1382

ITU-T

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
Ethernet over Transport aspects	G.8000–G.8099
MPLS over Transport aspects	**G.8100–G.8199**
Quality and availability targets (continuation of G.82x series)	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

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

ITU-T Recommendation G.8131/Y.1382

Linear protection switching for transport MPLS (T-MPLS) networks

Summary

ITU-T Recommendation G.8131/Y.1382 provides requirements and mechanisms for end-to-end trail and SNC protection switching for Transport MPLS (T-MPLS) networks. It describes the trail protection and SNC protection architectures types, the uni- and bidirectional switching types and the revertive/non-revertive operation types. It defines the automatic protection switching (APS) protocol used to align both ends of the protected domain.

Source

ITU-T Recommendation G.8131/Y.1382 was approved on 6 February 2007 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

APS, bridge, selector, SNC protection, T-MPLS, trail protection.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 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 expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. 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, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Introduction

This Recommendation specifies linear protection switching mechanisms to be applied to T-MPLS layer networks as described in G.8110.1/Y.1370.1. Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and bandwidth of the protection entity is reserved for a selected working entity. It provides a fast and simple survivability mechanism. It is easier for the network operator to grasp the status of the network (e.g., active network topology) with a protection switching than with other survivability mechanisms.

This Recommendation specifies 1+1 architecture and 1:1 architecture. The 1+1 architecture operates with unidirectional switching. The 1:1 architecture operates with bidirectional switching.

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

In the 1:1 architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity that carries the normal traffic. Since source and sink need to be coordinated to ensure that the selector bridge at the source and the selector at the sink select the same entity, an APS protocol is necessary.

ITU-T Recommendation G.8131/Y.1382

Linear protection switching for transport MPLS (T-MPLS) networks

1 Scope

This Recommendation provides architecture and mechanisms for trail and SNC/S protection switching for transport MPLS (T-MPLS) networks.

The APS protocol, 1+1 and 1:1 trail protection architecture and SNC/S protection architecture are defined in this version. Other protection architecture types are for further study.

This Recommendation describes the protection switching functionality for point-to-point connections.

Hitless protection switching is outside the scope of this version of the 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; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.805] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.808.1] ITU-T Recommendation G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection*.

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

3 Definitions

This Recommendation uses the following terms defined in ITU-T G.780/Y.1351:

3.1 bidirectional protection switching

3.2 unidirectional protection switching

This Recommendation uses the following terms defined in [ITU-T G.805]:

3.3 signal degrade (SD)

3.4 signal fail (SF)

3.5 trail

This Recommendation uses the following terms defined in ITU-T G.806:

3.6 defect

3.7 failure

This Recommendation uses the following terms defined in ITU-T G.870/Y.1352:

3.8 APS protocol

3.8.1 1-phase

3.8.2 2-phase

3.9 Protection class

3.9.1 individual

3.9.2 group protection

3.9.3 trail protection

3.10 Switch

3.10.1 forced switch

3.10.2 manual switch

3.11 Component

3.11.1 protected domain

3.11.2 bridge

3.11.2.1 permanent bridge

3.11.2.2 selector bridge

3.11.3 selector

3.11.3.1 selective selector

3.11.3.2 merging selector

3.11.4 sink node

3.11.5 source node

3.12 Architecture

3.12.1 1+1 protection architecture

3.12.2 1:n protection architecture

3.12.3 $(1:1)^n$ protection architecture

3.12.4 non-revertive (protection) operation

3.12.5 revertive (protection) operation

3.13 Signal

3.13.1 traffic signal

3.13.2 normal traffic signal

3.13.3 unprotected traffic signal

3.13.4 null signal

3.14 timers

3.14.1 hold-off time

3.14.2 wait-to-restore time

3.15 transport entities

3.15.1 protection transport entity

3.15.2 working transport entity

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APS	Automatic Protection Switching
DNR	Do Not Revert
EXER	Exercise
FDI	Forward Defect Indication
FS	Forced Switch
LP	Lockout of Protection
MPLS	Multiprotocol Label Switching
MS	Manual Switch
NR	No Request
OAM	Operation, Administration and Maintenance
PS	Protection Switching
RR	Reverse Request
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SF-P	Signal Fail for Protection
T-MPLS	Transport MPLS
TTSI	Trail Termination Source Identifier
WTR	Wait to Restore

5 Conventions

None.

6 Network objectives

The following network objectives apply:

1) *Switch time* – The APS algorithm for trail and SNC protection should operate as fast as possible. A value of 50 ms has been proposed as a target time. 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 protected scheme is for further study. Limitations on the transmission delay may be imposed if the target switch completion time for bidirectional protection switching operation is to be met. 1+1 unidirectional protection switching does not require transmission of APS signalling, so signalling transmission delays are not present.

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

4) *Extent of protection* – Trail and SNC protection should restore all traffic which has been interrupted due to a failure of a link connection which has been designated as forming part of a trail or an 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 trail or SNC.

5) *Switching types* – 1+1 trail and SNC protection should support unidirectional switching. 1:1 trail and SNC trail protection should support bidirectional protection switching.

6) *APS protocol and algorithm* – Both trail and SNC protection APS protocols should be identical for all network applications. APS is required for bidirectional switching only.

7) *Operation modes* – 1+1 unidirectional protection switching should support revertive operation, non-revertive operation, or both. 1:1 bidirectional protection switching should be revertive.

8) *Manual control* – Externally initiated commands may be provided for manual control of protection switching by the operations systems or craft. The following externally initiated commands should be supported: Clear, Lockout of Protection, Forced Switch, Manual Switch, Exercise.

9) *Switch initiation criteria* – Switch initiation criteria for trail protection should be identical to that for the corresponding SNC/S protection. The following automatically initiated commands shall be supported: Signal Failure – Working, Signal Failure – Protection, Signal Degrade – Working, Signal Degrade – Protection, Reverse Request, Wait To Restore, and No Request. The criteria for Signal Fail (SF) and/or Signal Degrade (SD) should be in harmony with definitions used in ITU-T Rec. G.8121/Y.1381.

7 Architecture types

Protection switching is a fully allocated protection mechanism that can be used on any topology. It is fully allocated in the sense that the route and bandwidth of the protection connection is reserved for a selected working connection. To be effective under all possible failures of the working connection however, the protection connection must be known to have complete physical diversity over all common-failure modes. This may not always be possible. Also, this might require the working connection not to follow its shortest path.

The T-MPLS protection switching architecture can be trail protection and SNC/S protection as defined in [ITU-T G.808.1]. Other types are for further study.

7.1 T-MPLS trail protection

T-MPLS trail protection is used to protect a T-MPLS connection. It is a dedicated end-to-end protection architecture, which can be used in different network structures, meshed networks, rings, etc.

7.1.1 1+1 trail protection

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

NOTE – To avoid a single point of failure, the working connection and the protection connection shall be routed along disjoint paths.

7.1.2 1:1 trail protection

In the 1:1 architecture type, a protection connection is dedicated to each working connection. The protected or working traffic is transmitted either by working or protection connection. The method for a selection between the working and protection connection depends on the mechanism.

NOTE – To avoid a single point of failure, the working connection and the protection connection shall be routed along disjoint paths.

7.2 T-MPLS SNC protection

T-MPLS subnetwork connection protection is used to protect a section of a connection (e.g., that section where two separate routes are available) within an operator's network or multiple operators' networks. Two independent subnetwork connections exist, which act as working and protection transport entities for the (protected) normal traffic signal.

7.2.1 SNC/S protection

The T-MPLS sub-layer trail termination functions (i.e., tandem connection termination functions) generate/insert and monitor/extract the T-MPLS OAM information to determine the status of the working and protection T-MPLS sublayer trails. See also [b-ITU-T G.8110.1 Amd.1]. APS information is transported over the protection SNC, except for the case of 1+1 unidirectional switching where APS is not supported.

8 Switching types

The protection switching types can be a unidirectional switching type or a bidirectional switching type.

8.1 Unidirectional switching type

In unidirectional switching, only the affected direction of the connection is switched to protection; the selectors at each end are independent. This type is applicable for 1+1 T-MPLS trail and SNC/S protection.

8.2 Bidirectional switching type

In bidirectional switching, both directions of the connection, including the affected direction and the unaffected direction, are switched to protection. For bidirectional switching, automatic protection switching (APS) protocol is required to coordinate the two endpoints. This type is applicable for 1:1 T-MPLS trail and SNC/S protection.

9 Operation types

The protection operation types can be a non-revertive operation type or a revertive operation type.

9.1 Non-revertive operation

In non-revertive types, the service will not be switched back to the working connection if the switch requests are terminated.

In non-revertive mode of operation, when the failed connection is no longer in an SF or SD condition, and no other externally initiated commands are present, a No Request state is entered. During this state, switching does not occur.

9.2 Revertive operation

In revertive types, the service will always return to (or remain on) the working connection if the switch requests are terminated.

In revertive mode of operation, under conditions where working traffic is being transmitted via the protection connection and when the working connection is restored, 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. Then, reversion back to select the working connection occurs. The Wait-to-Restore timer deactivates earlier if any local request of higher priority pre-empts this state.

10 Automatic protection switching (APS) protocol

Except for the case of 1+1 unidirectional switching, an APS signal is used to synchronize the action at the A and Z ends of the protected domain. Communicated are: Request/State type, Requested signal, Bridged signal, Protection configuration.

10.1 APS payload structure

The APS payload structure (see Table 10-1) in a T-MPLS OAM frame is for further study.

Table 10-1 – APS octets payload structure

1								2								3								4							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Request/ state				Protection type				Requested signal								Bridged signal								Reserved							
				A	B	D	R																								

The field values for the APS octets are defined in Table 10-2.

Table 10-2 – The fields values of APS channels

Field		Value	Description
Request/State		1111	Lockout of protection (LP)
		1110	Signal fail for protection (SF-P)
		1101	Forced switch (FS)
		1100	Signal fail (SF)
		1010	Signal degrade (SD)
		1000	Manual switch (MS)
		0110	Wait to restore (WTR)
		0100	Exercise (EXER)
		0010	Reverse request (RR)
		0001	Do not revert (DNR)
		0000	No request (NR)
		Others	Reserved for future international standardization
Protection type	A	0	No APS channel
		1	APS channel
	B	0	1+1 (Permanent bridge)
		1	$(1{:}1)^n$ (Selector bridge) ($n \geq 1$)
	D	0	Unidirectional switching
		1	Bidirectional switching
	R	0	Non-revertive operation
		1	Revertive operation
Requested signal		0	Null signal
		1-254	Normal traffic signal 1-254
		255	Unprotected traffic signal
Bridged signal		0	Null signal
		1-254	Normal traffic signal 1-254
		255	Unprotected traffic signal

10.2 APS protocol type

There are two basic requirements for APS protocol:

1) The prevention of misconnections.

2) The minimization of the number of communication cycles between A and Z ends of the protected domain, in order to minimize the protection switching time. The communication may be once (Z → A), twice (Z → A and A → Z), or three times (Z → A, A → Z and Z → A). This is referred to as 1-phase, 2-phase, and 3-phase protocols.

To keep balance between saving operational time, reducing protocol complexity and facilitating application, the suggested protocol types for the different protection architectures are shown in Table 10-3.

Table 10-3 – Protocol types related to protection architectures

Protocol type	Protection architecture
No protocol	1+1 unidirectional
1-phase APS	$(1:1)^n$ bidirectional ($n \geq 1$)

The details of the 1-phase APS protocol are for further study.

11 Application architectures

11.1 Unidirectional 1+1 trail protection switching

The 1+1 trail protection switching architecture is as shown in Figure 11-1. In the case of unidirectional protection switching operation as described here, protection switching is performed by the selector at the sink side of the protection domain based on purely local (i.e., protection sink) information. The working (protected) traffic is permanently bridged to the working and protection connection at the source side of the protection domain. If connectivity check packets are used to detect defects of the working and protection connection, they are inserted at the source of the protection domain of both working and protection side and detected and extracted at the sink side of the protection domain. It is noted that they should be sent regardless of whether the connection is selected by the selector or not.

Unidirectional 1+1 trail protection can be either revertive or non-revertive.

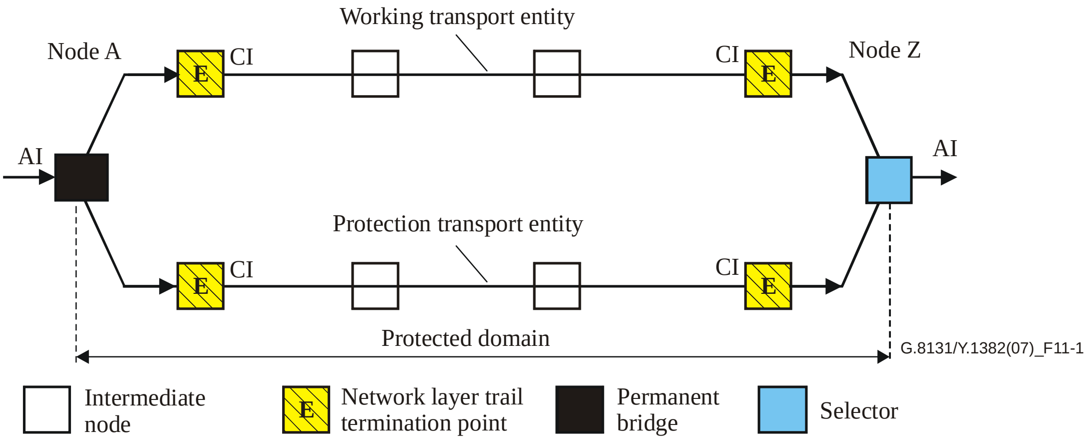

Figure 11-1 – Unidirectional 1+1 trail protection switching architecture

For example, if a unidirectional defect (in the direction of transmission from node A to node Z) occurs for the working connection as in Figure 11-2, this defect will be detected at the sink of the protection domain at node Z and the selector at node Z will switch to the protection connection.

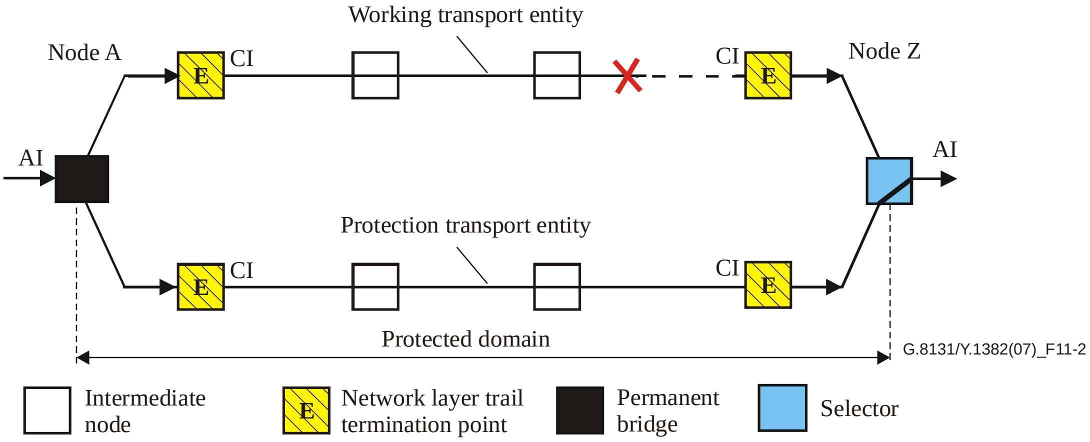

Figure 11-2 – Unidirectional 1+1 trail protection switching working connection fails

11.2 Bidirectional 1:1 trail protection switching

The 1:1 trail protection switching architecture is as shown in Figure 11-3. In the case of the bidirectional protection switching operation as described here, the protection switching is performed by both the selector bridge at the source side and the selector at the sink side of the protection domain based on local or near-end information and the APS protocol information from the other side or far end.

If connectivity check packets are used to detect defects of the working and protection connection, they are inserted at both working and protection side. It is noted that they should be sent regardless of whether the connection is selected by the selector or not.

Bidirectional 1:1 trail protection should be revertive.

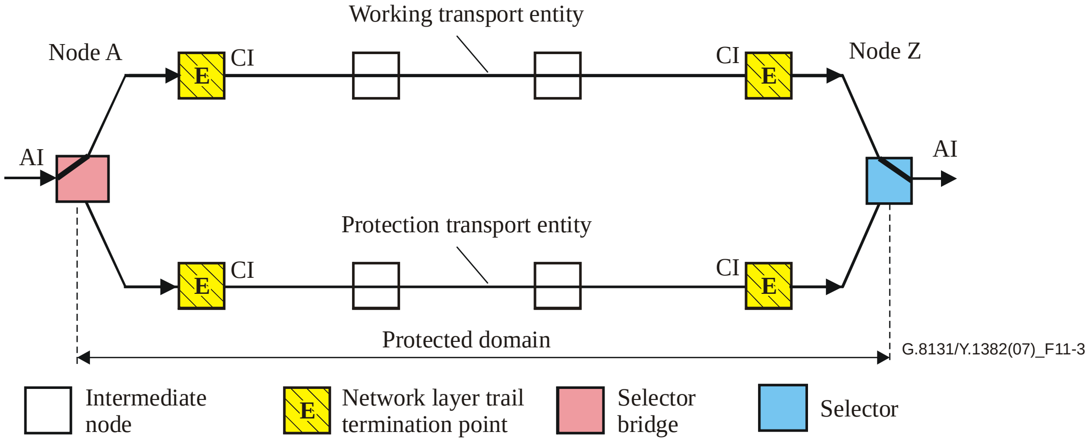

Figure 11-3 – Bidirectional 1:1 trail protection switching architecture unidirectional representation

For example, if a defect in the direction of transmission from node Z to node A occurs for the working connection Z-to-A as shown in Figure 11-4, this defect will be detected at node A. The APS protocol initiates the protection switching, a 1-phase APS protocol is used. The protocol is as follows:

- Node A detects the defect;
- The selector bridge at node A is switched to protection connection A-to-Z (i.e., in the A to Z direction the working traffic is sent on both working connection A-to-Z and protection connection A-to-Z) and the merging selector at node A switches to protection connection Z-to-A;
- The APS command sent from node A to node Z requests a protection switch;
- After node Z validates the priority of the protection switch request, the merging selector at node Z is switched to protection connection A-to-Z and the selector bridge at node Z is switched to protection connection Z-to-A (i.e., in the Z-to-A direction the working traffic is sent on both working connection Z-to-A and protection connection Z-to-A);
- Then, the APS command sent from node Z to node A is used to inform node A about the switching;
- Now, the traffic flows on the protection connection.

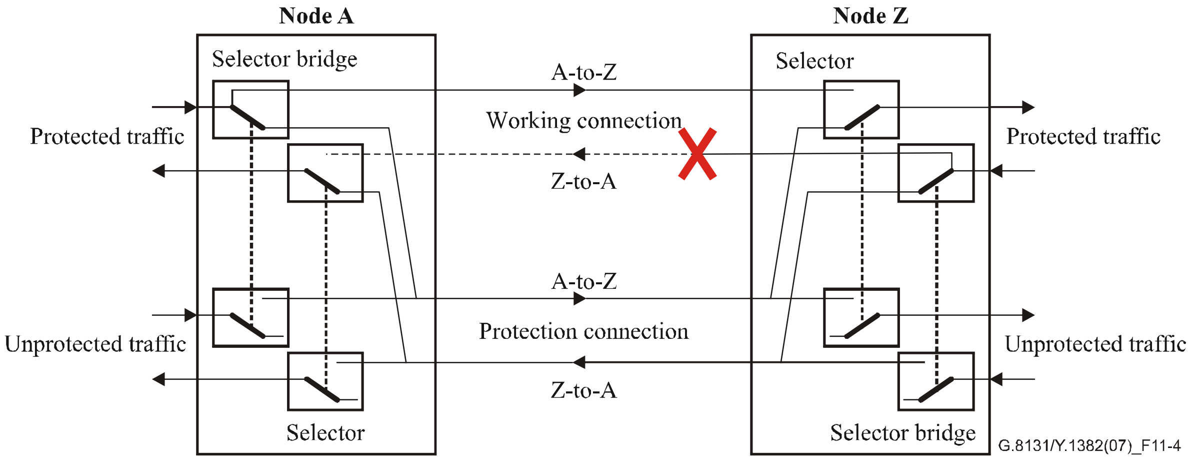

Figure 11-4 – Bidirectional 1:1 trail protection switching working connection Z-to-A fails

11.3 Unidirectional 1+1 SNC/S protection switching

The unidirectional 1+1 SNC/S protection switching architecture is as shown in Figure 11-5. In the case of unidirectional protection switching operation as described here, protection switching is performed by the selector at the sink (Node Z) of the protection domain based on purely local information. The working traffic is permanently bridged to working and protection connection at the source (Node A) of the protection domain. The server/sub-layer's trail termination and adaptation functions are used to monitor and determine the status of the working and protection connection. For the detailed protection switching mechanism, refer to the unidirectional 1+1 trail protection in clause 11.1.

Unidirectional 1+1 SNC/S protection can be either revertive or non-revertive.

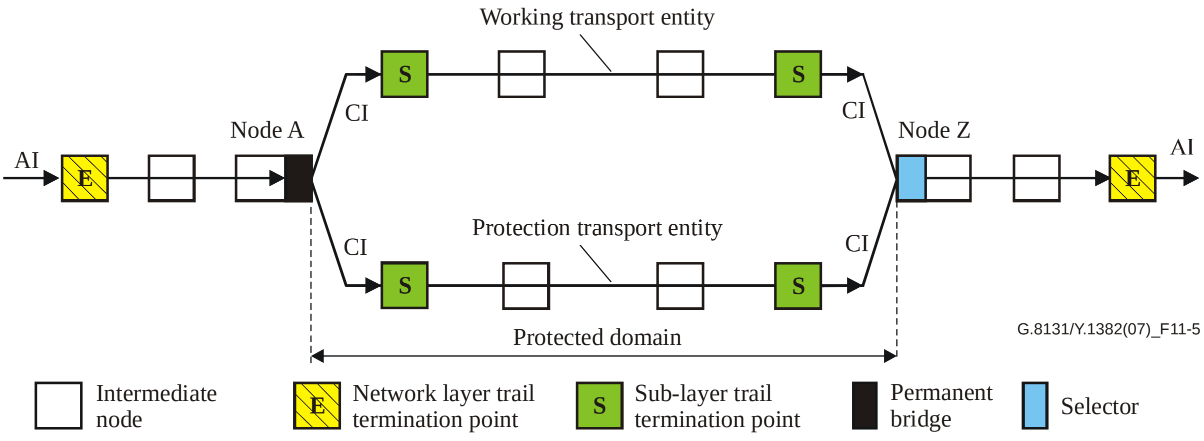

Figure 11-5 – Unidirectional 1+1 SNC/S protection switching architecture

11.4 Bidirectional 1:1 SNC/S protection switching

The bidirectional 1:1 SNC/S protection switching architecture is as shown in Figure 11-6. In the case of bidirectional protection switching operation as described here, the protection switching is performed by both the selector bridge at the source and the selector at the sink side of the protection domain based on local or near-end information and the APS protocol information from the other side or far end. The server/sub-layer's trail termination and adaptation functions are used to monitor and determine the status of the working and protection connection. For the detailed protection switching mechanism, refer to the bidirectional 1:1 trail protection in clause 11.2.

Bidirectional 1:1 SNC/S protection should be revertive.

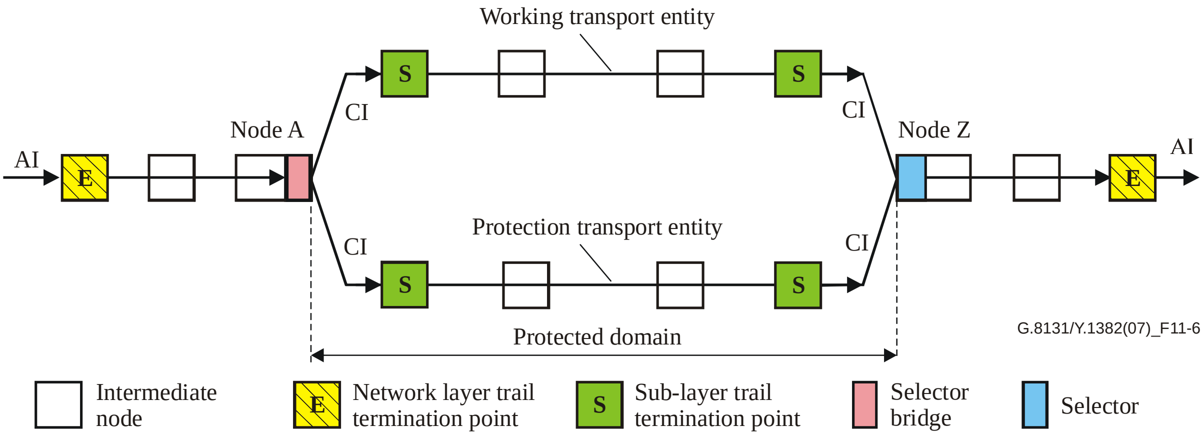

Figure 11-6 – Bidirectional 1:1 SNC/S protection switching architecture unidirectional representation

12 Protection switching trigger mechanism

Protection switching action shall be conducted when:

1) initiated by operator control (e.g., manual switch, forced switch, and lockout of protection) without a higher priority switch request being in effect;

2) SF or SD is declared on the associated connection (i.e., working connection or protection connection) and is not declared on the other connection and the hold-off timer has expired; or

3) the Wait-to-Restore timer expires (in revertive mode) and SF or SD is not declared on the working connection.

12.1 Manual control

Manual control of the protection switching function may be transferred from the element or network management system.

12.2 Signal fail declaration conditions

Signal fail (SF) is declared when the TMT_TT_Sk function detects a trail signal fail as defined in [b-ITU-T G.8110.1 Amd.1].

Signal Degrade (SD) is declared when the TMT_TT_Sk function detects a trail signal degrade as defined in [b-ITU-T G.8110.1 Amd.1].

13 APS switch initiation criteria

The following switch initiation criteria exist:

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

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

3) a state (Wait to Restore, Reverse Request, Do Not Revert, No Request) of the protection switching function.

The priority of request/state is given in Table 13-1. In the case of unidirectional switching, the priority is determined at the near end only. In bidirectional switching, the local request will be indicated only in the case where it is as high or higher than any request received from the far end via the APS channel. In bidirectional switching, when the far-end request has the highest priority, the near end will signal Reverse Request.

Table 13-1 – Priority of request/state

Local request	Order of priority
Clear	Highest
Lockout of Protection (LP)	|
Signal Fail for Protection (SF-P)	|
Forced Switch (FS)	|
Signal Fail (SF)	|
Signal Degrade (SD)	|
Manual Switch (MS)	|
Wait To Restore (WTR)	|
No Request (NR)	Lowest

13.1 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 (LP): Fix the selector position to the working connection. Prevents the selector from switching to the protection connection when it is selecting the working connection. Switches the selector from the protection to the working connection when it is selecting the protection connection.

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

Manual Switch (MS) for working connection: Switches the selector from the working connection to the protection connection, unless an equal or higher priority switch request (i.e., LP, FS, SF or MS) is in effect.

Manual Switch (MS) for protection connection: Switches the selector from the protection connection to the working connection, unless an equal or higher priority switch request (i.e., LP, FS, SF or MS) is in effect.

13.2 States

Wait to Restore: This state is only applicable for the revertive mode and applies to a working connection. This state is entered by the local protection switching function in conditions where working traffic is being received via the protection connection when the working connection is restored, if local protection switching requests have been previously active and now become inactive. It prevents reversion back to select the working connection until the Wait-to-Restore timer has expired. The Wait-to-Restore time may be configured by the operator in 1-minute steps between 5 and 12 minutes; the default value is 5 minutes. An SF or SD condition will override the WTR.

No Request: This state is entered by the local protection switching function under all conditions where no local protection switching requests (including Wait to Restore) are active.

14 Security aspects

This Recommendation does not raise any security issues that are not already present in either the T-MPLS architecture or in the architecture of its client layer protocols.

Protection switching could enhance the security of T-MPLS networks as it will automatically switch traffic from defective connections that may have been misbranched or misconfigured into other connections, onto proper working connections. This will prevent customers' traffic being exposed to other customers.

Appendix I

Selector types

(This appendix does not form an integral part of this Recommendation)

There are two possible implementations of a selector: the selective selector or the merging selector. Both provide the same behaviour.

I.1 Selective selector

For further study.

I.2 Merging selector

For further study.

Bibliography

[b-ITU-T G.8113]	ITU-T Recommendation G.8113/Y.1372 (2007), *Requirements for OAM functions in T-MPLS-based networks*.
[b-ITU-T G.8114]	ITU-T Recommendation G.8114/Y.1373 (2007), *Operation and maintenance mechanism for T-MPLS layer networks*.
[b-ITU-T G.8110.1 Amd.1]	ITU-T Recommendation G.8110.1/Y.1370.1 (2006), *Architecture of Transport MPLS (T-MPLS) layer network* – Amendment 1.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Cable networks and 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	Telecommunication management, including TMN and network maintenance
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, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007