International Telecommunication Union

ITU-T G.8131/Y.1382

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Amendment 1

(09/2007)

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

Amendment 1

ITU-T Recommendation G.8131/Y.1382 (2007) – Amendment 1

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	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

Amendment 1

Summary

Amendment 1 to ITU-T Recommendation G.8131/Y.1382 contains additional material to be incorporated into ITU-T Recommendation G.8131/Y.1382, *Linear protection switching for transport MPLS (T-MPLS) networks*. It presents further specification of the APS protocol.

Source

Amendment 1 to ITU-T Recommendation G.8131/Y.1382 (2007) was approved on 22 September 2007 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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/.

ITU-T Recommendation G.8131/Y.1382

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

Amendment 1

Modifications introduced by this amendment are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged texts (clause numbers, etc.) may be kept to indicate the correct insertion points.

• • •

6 Network objectives

• • •

10) *Mismatch detection* – A mismatch between the bridge/selector positions of the near end and the far end should be detected.

– The bridge/selector mismatch for the local network element should be detected and reported.

– The bridge/selector mismatch should be cleared by a network operator.

7 Protection a~~A~~rchitecture ~~types~~ and characteristics

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 linear 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. That means the client layer of a T-MPLS protected domain is also a T-MPLS layer (TMC or TMP). 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~~provisioned 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~~provisioned along disjoint paths.

7.2 T-MPLS SNC protection

• • •

~~8~~7.3 Switching types

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

~~8.1~~7.3.1 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~~7.3.2 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~~7.4 Operation types

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

~~9~~7.4.1 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~~7.4.2 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.

• • •

[Clause 12 has been moved and renumbered as clause 7.5.]

~~12~~7.5 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~~.~~;

4) in the bidirectional 1:1 architecture, the received APS protocol requests to switch and it has a higher priority than any other local request.

~~12~~7.5.1 Manual control

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

~~12~~7.5.2 Signal fail declaration conditions

Protection switching will occur based on the detection of certain defects on the transport entities (working and protection) within the protected domain. How these defects are detected is the subject of the equipment Recommendations (e.g., ITU-T Rec. G.8121/Y.1381). For the purpose of the protection switching process, a transport entity within the protected domain has a condition of OK, failed (signal fail = SF), or degraded (signal degrade = SD) if applicable.

In Trail protection switching,

Signal fail (SF) is declared when the TM~~T~~_TT_Sk function in the protected domain detects a trail signal fail as defined in ~~[b-ITU-T G.8110.1 Amd.1]~~ITU-T Rec. G.8121/Y.1381.

Signal Degrade (SD) is declared when the TM~~T~~_TT_Sk function in the protected domain detects a trail signal degrade as defined in ~~[b-ITU-T G.8110.1 Amd.1]~~ ITU-T Rec. G.8121/Y.1381.

In SNC/S protection switching,

Signal Fail (SF) is declared when the TMT_TT_Sk function in the protected domain detects a trail signal fail as defined in ITU-T Rec. G.8121/Y.1381.

Signal Degrade (SD) is declared when the TMT_TT_Sk function in the protected domain detects a trail signal degrade as defined in ITU-T Rec. G.8121/Y.1381.

7.6 Provisioning mismatches

With all of the options for provisioning of protection groups, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of several forms:

– Mismatches where proper operation is not possible.

– Mismatches where one or both sides can adapt their operation to provide a degree of interworking in spite of the mismatch.

– Mismatches that do not prevent interworking. An example is the revertive/non-revertive mismatch discussed in clauses 7.4 and 9.4.

Not all provisioning mismatches can be conveyed and detected by information passed through the APS communication. There are simply too many combinations of valid entity numbers to easily provide full visibility of all of the configuration options. What is desirable, however, is to provide visibility for the middle category, where the sides can adapt their operation to interwork in spite of the mismatch. The user could still be informed of the provisioning mismatch, but a level of protection could still be provided by the equipment.

8 Protection group commands and states

[Clause 13.1 has been moved and renumbered as clause 8.1.]

~~13~~8.1 Externally initiated commands

• • •

8.2 Local commands

These commands apply only to the near end of the protection group. Even when an APS protocol is supported, they are not signalled to the far end.

Lockout-normal-traffic signal from protection – Prevents normal traffic signal from being selected from the protection entity. Commands for normal traffic signal will be rejected. For normal traffic, any indication of SF (or SD if applicable) will be ignored. In bidirectional switching, remote bridge requests for normal traffic signal will still be honoured to prevent protocol failures. As a result, a normal traffic signal must be locked out from the protection transport entity at both ends to prevent it being selected from the protection transport entity as a result of a command or failure at either end.

Clear lockout-normal-traffic signal from protection

[Clause 13.2 has been moved and renumbered as clause 8.3.]

~~13.2~~8.3 States

• • •

~~10~~9 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.~~

The only switching type that does NOT require APS protocol is 1+1 unidirectional switching. With a permanent bridge at the head end and no need to coordinate selector positions at the two ends, the tail end selector can be operated entirely according to defects and commands received at the tail end.

Bidirectional switching always requires APS protocol.

~~10~~9.1 APS ~~payload~~ information 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 ≥ 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

APS-specific information is transmitted within specific fields in the APS PDU that is one of a suite of T-MPLS OAM PDUs defined in [b-ITU-T G.8114]. Four octets in the APS PDU are used to carry APS-specific information. In addition, it should be noted that the TLV Offset field in the APS PDU is set to 0x04.

The format of the APS-specific information is defined in Figure 9-1.

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

Figure 9-1 – APS octets payload structure

Table 9-1 describes code points and values for APS-specific information.

Table 9-1 – The fields values of APS channels

Field		Value	Description	Priority
Request/State		1111	Lockout of Protection (LO)	highest
		1110	Signal Fail for Protection (SF-P)	↑
		1101	Forced Switch (FS)	¦
		1011	Signal Fail for Working (SF)	¦
		1001	Signal Degrade (SD) – (Note 1)	¦
		0111	Manual Switch (MS)	¦
		0101	Wait-to-Restore (WTR)	¦
		0100	Exercise (EXER) – (Note 2)	¦
		0010	Reverse Request (RR) – (Note 3)	¦
		0001	Do Not Revert (DNR)	↓
		0000	No Request (NR)	lowest
		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 (Selector Bridge)	
	D	0	Unidirectional switching	
		1	Bidirectional switching	
	R	0	Non-revertive operation	
		1	Revertive operation	
Requested Signal		0	Null Signal	
		1	Normal Traffic Signal	
		2-255	Reserved for future use	
Bridged Signal		0	Null Signal	
		1	Normal Traffic Signal	
		2-255	Reserved for future use	

NOTE 1 – SD is for further study.
NOTE 2 – EXER is for further study.
NOTE 3 – RR is for further study.

[Clause 13 has been moved and renumbered as clause 9.1.1.]

~~13~~9.1.1 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~~

~~10~~9.2 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~~9-2.

Table ~~10-3~~9-2 – Protocol types related to protection architectures

Protocol type	Protection architecture
No protocol	1+1 unidirectional
1-phase APS	~~(~~1:1~~)~~[a] bidirectional ~~(n ≥ 1)~~

NOTE – The use of a "1-phase" protocol implies that the "label distribution policy" assigns a unique label value per path, in such a way that it avoids different LSPs to access the protection resource (even in transient phases) with the same label. A unique label per path allows avoiding misconnections.

The details of the 1-phase APS protocol are ~~for further study~~ in clause 9.4.

9.3 Transmission and acceptance of APS

APS signals are transported via the protection transport entity only, being inserted by the head end of the protected domain and extracted by the tail end of the protected domain.

A new APS signal must be transmitted immediately when a change in the transmitted status occurs.

The first three APS signals should be transmitted as fast as possible only if the APS information to be transmitted has been changed so that fast protection switching is possible even if one or two APS signals are lost or corrupted. For the fast protection switching in 50 ms, the interval of the first three APS signals should be 3.3 ms. APS signals after the first three should be transmitted with the interval of 5 seconds.

If no valid APS specific information is received, the last valid received information remains applicable. In the event a signal fail condition is detected on the protection transport entity, the received APS specific information should be evaluated.

If a protection end point receives APS specific information from the working entity, it should ignore this information, and should detect the failure of protocol defect for the local network element (see clause 9.17).

9.4 1-phase APS protocol

9.4.1 Principle of operation

Figure 9-2 illustrates the principle of the linear protection switching algorithm. This algorithm is performed in network elements at both ends of the protected domain. Bidirectional switching is achieved by transmitting local switching requests to the far end via the "Request/State" in the first octet of the APS-specific information (see Table 9-1). The transmitted "Requested Signal" and "Bridged Signal" in the second and the third octets of the APS-specific information contain the local bridge/selector status information; a persistent mismatch between both ends may thus be detected and leads to an alarm.

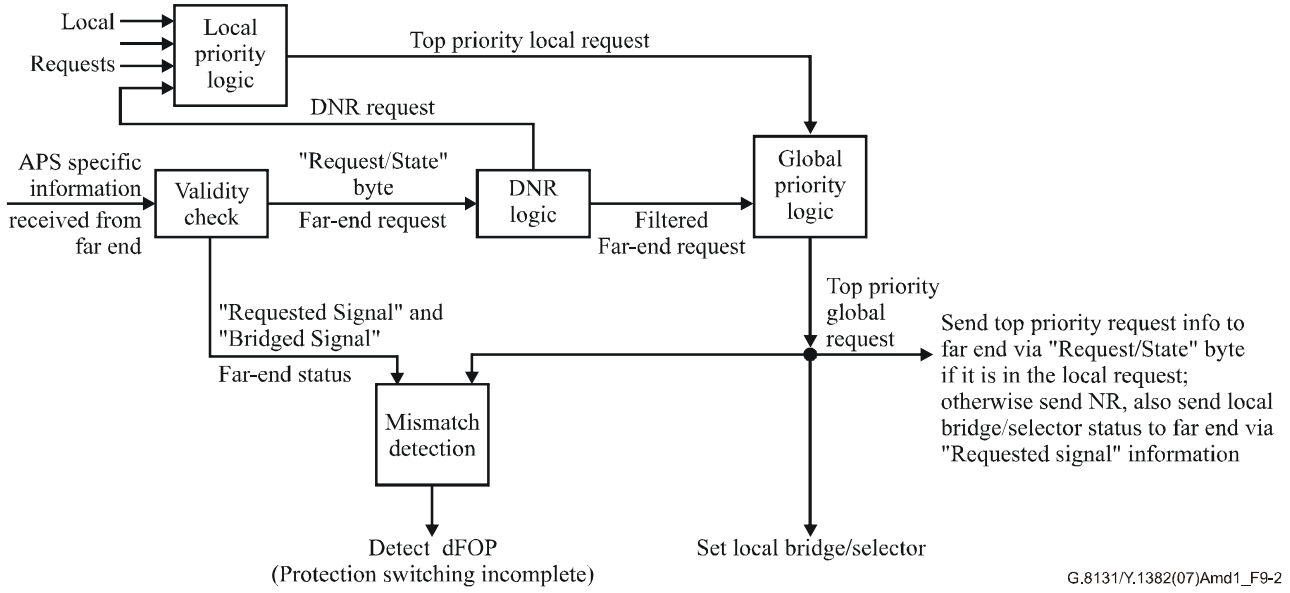

Figure 9-2 – Principle of linear protection switching algorithm

In detail, the functionality is as follows (see Figure 9-2):

At the local network element, one or more local protection switching requests (as listed in clauses 8.1 and 8.2) may be active. The "local priority logic" determines which of these requests is of top priority, using the order of priority given in Table 9-1. This top priority local request information is passed on to the "global priority logic".

The local network element receives information from the network element of the far end via the APS-specific information. The received APS-specific information is subjected to a validity check (see clause 9.3). The information of the received "Request/State" information (which indicates the top priority local request of the far end) is then passed on to the "DNR logic". If the received "Request/State" information is DNR, then it is filtered by "DNR logic". "DNR logic" then generates DNR if the received "Request/State" information is DNR. The generated local request is then passed to "local priority logic". If the received "Request/State" information is not DNR, it is simply passed to "global priority logic". The "global priority logic" compares the top priority local request with the request of the received "Request/State" information (according to the order of priority of Table 9-1) to determine the top priority global request. If the top priority global request is the local request, it will be indicated in "Request/State" field, otherwise "NR" will be indicated. The top priority global request will be exactly the same as the top priority local request in the case of unidirectional protection switching because the received "Request/State" information should not affect the operation of the unidirectional protection switching. This request then determines the bridge/selector position (or status) of the local network element as follows:

– for 1+1 architectures, only the selector position is controlled. For 1:1 architectures, both the bridge and the selector positions are maintained to select the same position;

– if the top priority global request is a request for a working entity, the associated working traffic is bridged/switched to/from the protection entity, i.e., the associated bridge/selector of the local network element selects the protection entity. A switching request for a working entity means a request to switch from a working entity to the protection entity.

The bridge/selector status is transmitted to the far end via the "Request Signal" and "Bridged Signal" (with coding as described in Table 9-1). It is also compared with the bridge/selector status of the far end as indicated by the received "Request Signal" and "Bridged Signal". Note that the linear protection switching algorithm commences immediately every time one of the input signals (see Figure 9-2) changes, i.e., when the status of any local request changes, or when a different APS-specific information 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 APS-specific information (if necessary), or detect dFOP if the protection switching is not completed within a period specified in clause 9.17.

9.4.2 Revertive mode

In revertive mode of unidirectional protection switching operation in 1-phase APS, in conditions where working traffic is being received via the protection entity, if local protection switching requests (see Figure 9-2) 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 "Request/State" information and maintains the switch.

In the case of bidirectional protection switching, a local wait-to-restore state is entered only when there is no higher priority of request received from the far end than that of the wait-to-restore state.

This state normally times out and becomes a no request state after the wait-to-restore timer has expired. The wait-to-restore timer is deactivated earlier if any local request of higher priority pre-empts this state.

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 "Request/State" information. 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.

9.4.3 Non-revertive mode

In non-revertive mode of unidirectional protection switching operation in 1-phase APS, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests (see Figure 9-2) 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 "Request/State" information and maintains the switch, thus preventing reversion back to the released bridge/selector position in non-revertive mode under no request conditions.

In the case of bidirectional protection switching operation, a local do not revert state is entered only when there is no higher priority of request received from the far end than that of the do not revert state.

9.5 Request type

These requests reflect the highest priority condition, command or state. In the case of unidirectional switching, this is the highest priority value determined from the near end only. In bidirectional switching, the local request will be indicated only in the case where it is as high as or higher than any request received from the far end over the APS communication, otherwise NR will be indicated. In 1-phase APS protocol, the near end will never signal Reverse Request even when the far end request has the highest priority.

9.6 Protection types

The valid protection types (bits ABDR) are:

000x 1+1 Unidirectional, no APS communication
1111 1:1 Bidirectional with APS communication, revertive

The values are chosen such that the default value (all zeros) matches the only type of protection that can operate without APS (1+1 unidirectional).

If the "B" bit mismatches, the selector is released since 1:1 and 1+1 are incompatible. This will result in a defect.

Provided the "B" bit matches:

The "A" bit, implicitly, shall not mismatch:
The "D" bit, implicitly, shall not mismatch.

When the B bit matches and B = 0 (1+1), it is possible to have one side revertive and the other side non-revertive (R bit mismatch) as indicated by the "x".

When the B bit matches and B = 1 (1:1), only revertive switching is supported and therefore the "R" bit, implicitly, shall not mismatch.

9.7 Requested signal

This indicates the signal that the near end requests be carried over the protection path. For NR, this is the null signal when the far end is not bridging normal traffic signal to the protection entity. When the far end is bridging normal traffic signal to the protection entity, the requested signal is the normal traffic signal for NR; for LO, this can only be the null signal. For SF (or SD if applicable), this will be the normal traffic signal, or the null signal to indicate that protection has failed or has

been degraded. For all other requests, this will be the normal traffic signal requested to be carried over the protection transport entity.

9.8 Bridged signal

This indicates the signal that is bridged onto the protection path. For 1+1 protection, this should always indicate the normal traffic signal, accurately reflecting the permanent bridge. For 1:1 protection, this will indicate what is actually bridged to the protection entity (either the null signal, or normal traffic signal). This will generally be the bridge requested by the far end.

9.9 Control of bridge

In 1+1 architectures, the normal traffic signal is permanently bridged to protection. The normal traffic signal will always be indicated in the bridged signal field of the APS information.

In 1:1 architectures, the bridge will be set to the one indicated by the "Requested Signal" field of the incoming APS information. Once the bridge has been established, this will be indicated in the "Bridged Signal" field of the outgoing APS information.

9.10 Control of selector

In 1+1 unidirectional architectures (with or without APS communication), the selector is set entirely according to the highest priority local request. This is a single phase switch.

In 1:1 bidirectional architectures, normal traffic signal will be selected from the protection entity when the number appears in the outgoing "Requested Signal".

9.11 Signal fail of the protection transport entity

Signal Fail on the protection transport entity has a higher priority than any defect that would cause a normal traffic signal to be selected from protection. In 1-phase APS an SF-P on the protection transport entity (over which the APS signal is routed) has priority over the Forced Switch. Lockout command has higher priority than SF-P: during failure conditions, lockout status shall be kept active.

9.12 Equal priority requests

In general, once a switch has been completed due to a request, it will not be overridden by another request of the same priority (first come, first served behaviour). Equal priority requests from both sides of a bidirectional protection group are both considered valid.

9.13 Command acceptance and retention

The commands CLEAR, LO, FS, MS and EXER are accepted or rejected in the context of previous commands, the condition of the working and protection entities in the protection group, and (in bidirectional switching only) the received APS information.

The CLEAR command is only valid if a near end LO, FS, MS or EXER command is in effect, or if a WTR state is present at the near end and rejected otherwise. This command will remove the near end command or WTR state, allowing the next lower priority condition or (in bidirectional switching) APS request to be asserted.

Other commands are rejected unless they are higher priority than the previously existing command, condition, or (in bidirectional switching) APS request. If a new command is accepted, any previous, lower priority command that is overridden is forgotten. If a higher priority command overrides a lower priority condition or (in bidirectional switching) APS request, that other request will be reasserted if it still exists at the time the command is cleared.

If a command is overridden by a condition or (in bidirectional switching) by an APS request, that command is forgotten.

9.14 Hold-off timer

In order to coordinate timing of protection switches at multiple layers or across cascaded protected domains, a hold-off timer may be required. The purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protected domain to switch before a downstream domain (e.g., to allow an upstream ring to switch before the downstream ring in a dual node interconnect configuration so that the switch occurs in the same ring as the failure).

Each protection group should have a provisionable hold-off timer. The suggested range of the hold-off timer is 0 to 10 seconds in steps of 100 ms.

When a new defect or more severe defect occurs (new SF (or SD if applicable)), this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked whether a defect still exists on the trail that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

9.15 Wait-to-restore timer

In revertive mode of operation, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become fault-free. After the failed working transport entity meets this criterion, a fixed period of time shall elapse before a normal traffic signal uses it again. This period, called wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 0 and 12 minutes; the default value is 5 minutes. An SF (or SD if applicable) condition will override the WTR.

In revertive mode of operation, when the protection is no longer requested, i.e., the failed working transport entity is no longer in SF (or SD if applicable) condition (and assuming no other requesting transport entities), a local wait-to-restore state will be activated. Since this state becomes the highest in priority, it is indicated by the APS signal (if applicable), and maintains the normal traffic signal from the previously failed working transport entity on the protection transport entity. This state shall normally time out and become a no request state. The wait-to-restore timer is stopped before it expires when any request of higher priority pre-empts this state.

9.16 Exercise operation

The Exercise operation is for further study.

9.17 Failure of protocol defects

"Failure of Protocol" situations for protection types requiring APS are as follows:

– Fully incompatible provisioning (the "B" bit mismatch, described in clause 9.6);

– Working/Protection configuration mismatch (described in clause 9.3);

– Lack of response to a bridge request (i.e., no match in sent "Requested Signal" and received "Requested Signal") for > 50 ms.

Fully incompatible provisioning and working/protection configuration mismatch are detected by receiving only one APS frame. Detection and clearance of "Failure of Protocol" defects are defined in ITU-T Rec. G.8121/Y.1381.

If an unknown request or a request for an invalid signal number is received, it will be ignored.

9.18 Signal degrade processing

The protection switching controller does not care which monitoring method is used, as long as it can be given (OK, SF, SD if applicable) information for the transport entities within the protected domain. Some monitors or network layers may not have an SD detection method. Where this is the case, there is no need to use a different APS protocol: it would simply happen that an SD would not be issued from equipment that cannot detect it. Where an APS protocol is used, the implementation should not preclude the far end from declaring an SD over the APS protocol, even if the monitor at the near end cannot detect SD.

11 0 Application architectures

11 0.1 Unidirectional 1+1 trail protection switching

The 1+1 trail protection switching architecture is as shown in Figure 11 0-1. 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 (transport entity) at the source side of the protection domain. If ~~connectivity check~~ Continuity and Connectivity Check OAM 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.

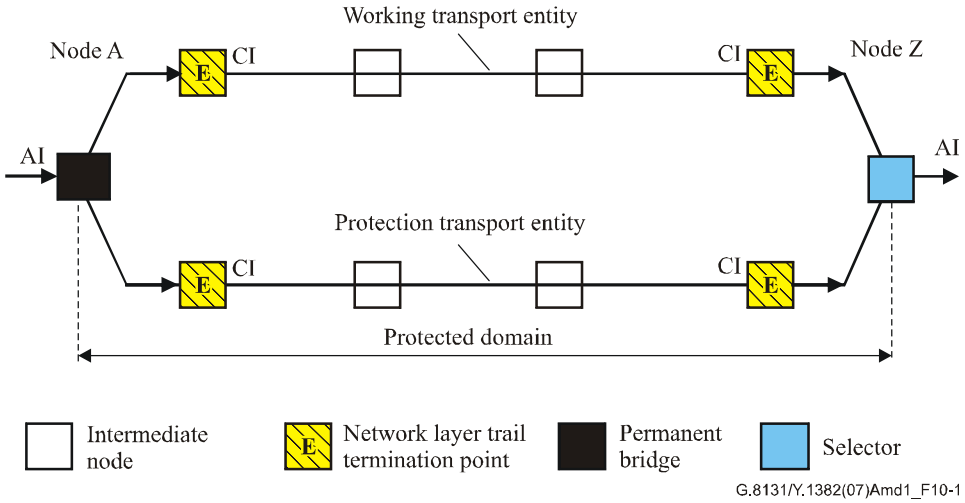

Figure 11 0-1 – Unidirectional 1+1 trail protection switching architecture

For example, if a unidirectional defect (in the direction of transmission from node A to node Z) occurs for the working connection (transport entity) as in Figure 11 0-2, 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.

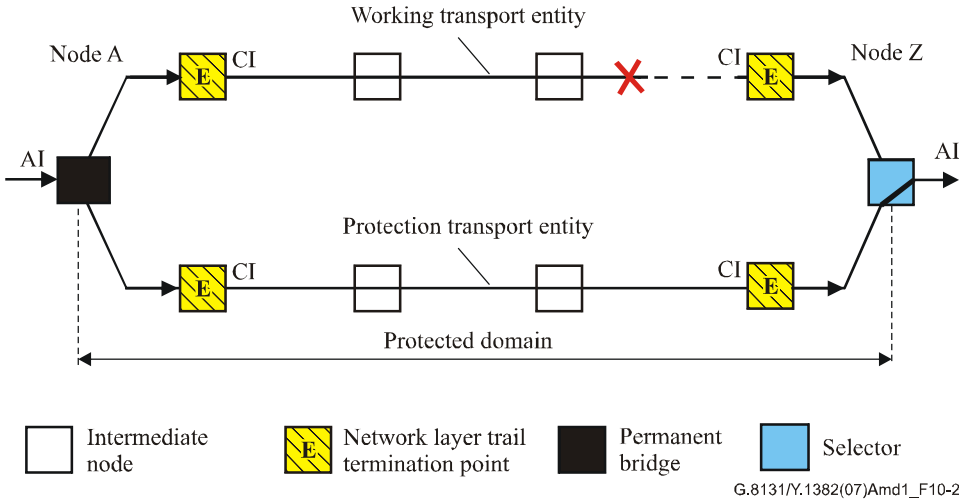

Figure 1~~1~~0-2 – Unidirectional 1+1 trail protection switching working connection fails

1~~1~~0.2 Bidirectional 1:1 trail protection switching

The 1:1 trail protection switching architecture is as shown in Figure 1~~1~~0-3. 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~~ Continuity and Connectivity Check OAM 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.

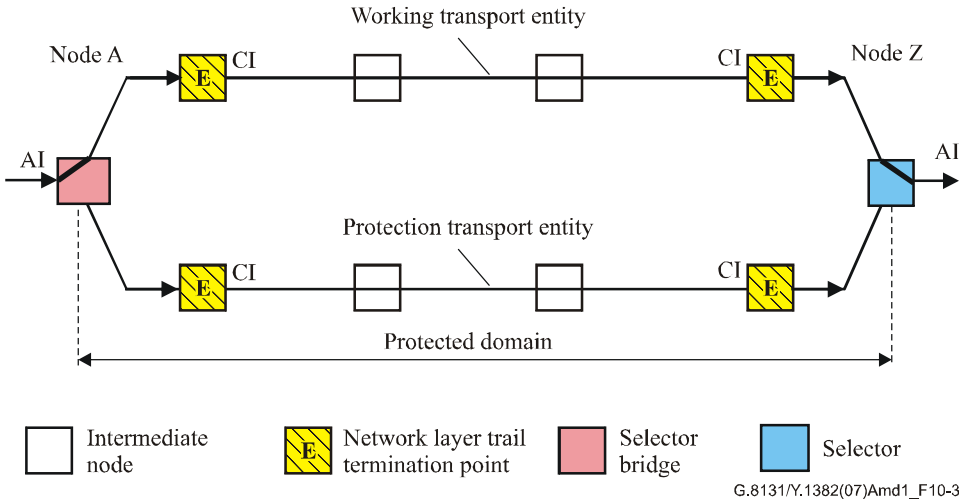

Figure 1~~1~~0-3 – Bidirectional 1:1 trail protection switching architecture unidirectional representation

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 1~~1~~0-4, 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~~ protection 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.

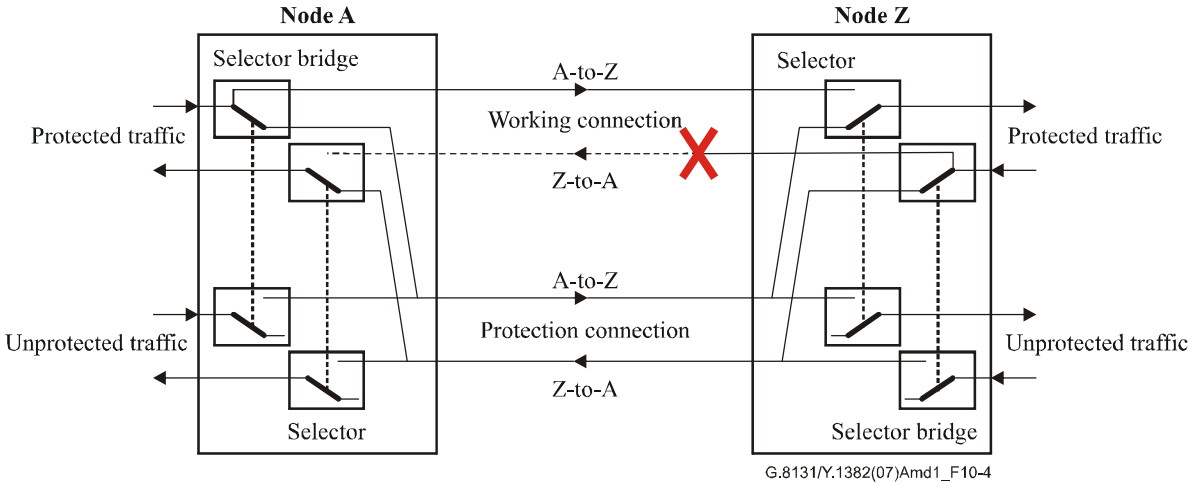

Figure 1~~1~~0-4 – Bidirectional 1:1 trail protection switching working connection Z-to-A fails

1~~1~~0.3 Unidirectional 1+1 SNC/S protection switching

The unidirectional 1+1 SNC/S protection switching architecture is as shown in Figure 1~~1~~0-5. 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 (transport entity) 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 1~~1~~0.1.

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

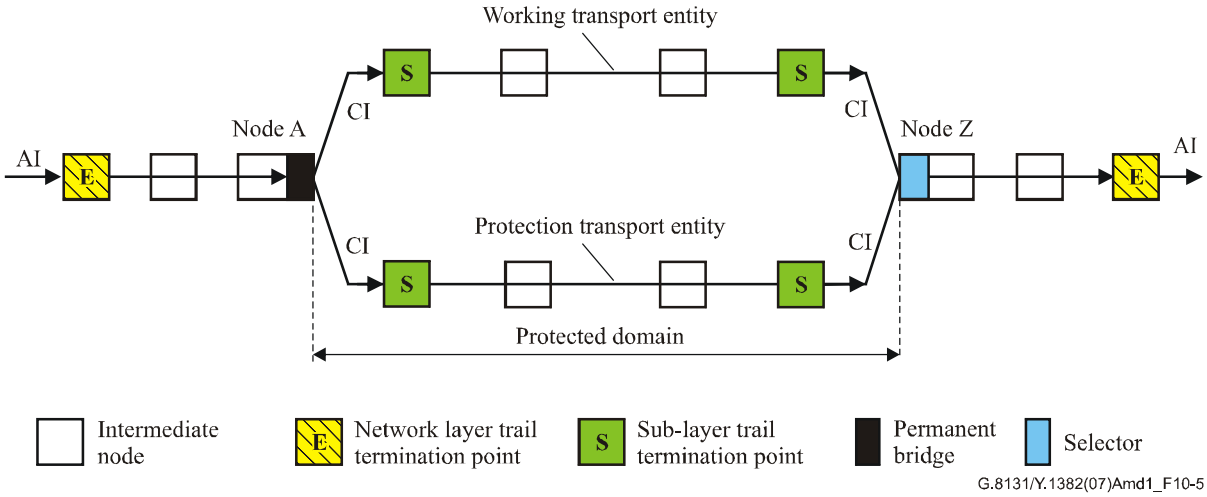

Figure 1~~1~~0-5 – Unidirectional 1+1 SNC/S protection switching architecture

1~~1~~0.4 Bidirectional 1:1 SNC/S protection switching

The bidirectional 1:1 SNC/S protection switching architecture is as shown in Figure 1~~1~~0-6. 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 1~~1~~0.2.

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

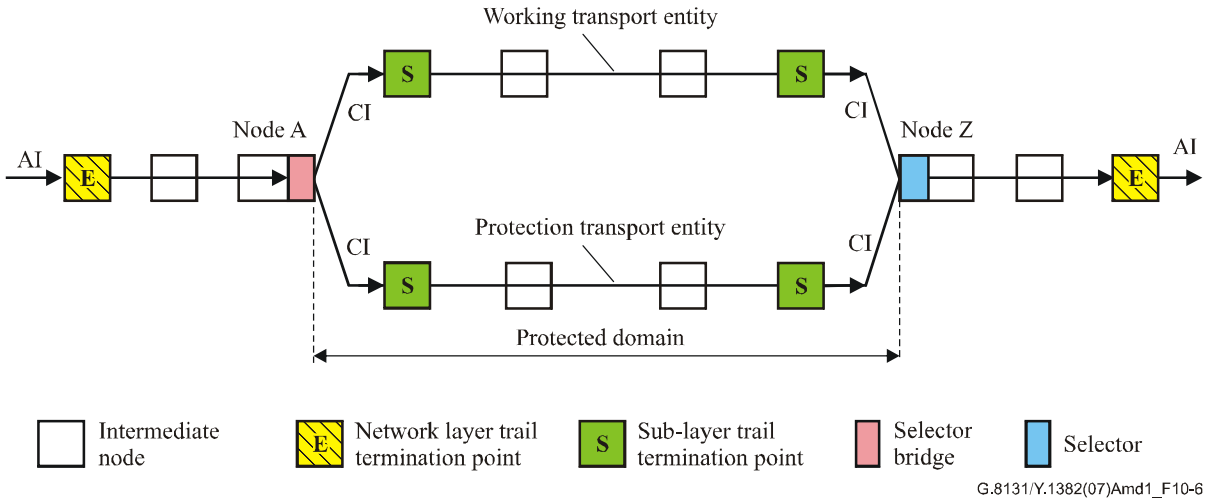

Figure 1~~1~~0-6 – Bidirectional 1:1 SNC/S protection switching architecture unidirectional representation

14<u>1</u> 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.

Annex A

State transition tables of protection switching

(This annex forms an integral part of this Recommendation)

In this annex, state transition tables for the following protection switching configurations are described.

– 1:1 bidirectional (revertive mode)

– 1+1 unidirectional (revertive mode, non-revertive mode)

NOTE – The state SD and the requests EXER and RR are for further study. This is indicated in the following tables by highlighted cells: TBD

A.1 State transition for 1:1 bidirectional switching with revertive mode

A.1.1 Local Requests

Table A.1 shows the state transition by a local request for the 1:1 protection switching in revertive mode.

A.1.2 Far End Requests

Table A.2 shows the state transition by a far end request received by APS for the 1:1 bidirectional protection switching in revertive mode.

A.2 State transition for 1+1 unidirectional switching with revertive mode

A.2.1 Local Requests

Table A.3 shows the state transition by a local request for the 1+1 unidirectional protection switching in revertive mode.

A.3 State transition for 1+1 unidirectional switching with non-revertive mode

A.3.1 Local Requests

Table A.4 shows the state transition by a local request for the 1+1 unidirectional protection switching in non-revertive mode.

Table A.1 – State Transition by Local Requests (1:1, bidirectional, revertive mode)

State		Signalled APS	Local request													
			a	b	c	d	e	f	g	h	i	j	k	l	m	n
			Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	SD on working	Working recovers from SD	SD on protection	Protection recovers from SD	Manual switch	Clear	Exercise	WTR timer expires
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E[a]	N/A	→F	N/A	TBD	TBD	TBD	TBD	→I	O	TBD	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B)[b] or →E	O	→F	N/A	TBD	TBD	TBD	TBD	→I	O	TBD	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	TBD	TBD	TBD	TBD	O	→A or →E[c] →F[d]	TBD	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	TBD	TBD	TBD	TBD	O	→A or →E[c]	TBD	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→J	→F	N/A	TBD	TBD	TBD	TBD	O	O	TBD	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	TBD	TBD	TBD	TBD	O	O	TBD	N/A
G	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
H	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
I	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	TBD	TBD	TBD	TBD	O	→A	TBD	N/A
J	Wait-to-Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	TBD	TBD	TBD	TBD	→I	→A	TBD	→A
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
L	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or lower priority.
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
[a] It transits to the state E if the Signal Fail still exists after hold-off timer expires. [b] If FS is indicated in the received APS from the far end. [c] If SF is reasserted. [d] If SF-P is reasserted.

Table A.2 – State transition by Far End Requests (1:1, bidirectional, revertive mode)

State		Signalled APS	Received far end request											
			o	p	q	r	s	t	u	v	w	x	y	z
			LO [r/b=null]	SF-P [r/b=null]	FS [r/b= normal]	SF [r/b= normal]	SD [r/b=null]	SD [r/b= normal]	MS [r/b= normal]	WTR [r/b= normal]	EXER [r/b=null]	RR [r/b=null]	NR [r/b=null]	NR [r/b= normal]
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	TBD	TBD	→B	N/A	TBD	TBD	(→A) or →E[a] or →F[b]	(→A)
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	TBD	TBD	(→B)	(→B)	TBD	TBD	→A or →E[a]	→A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	TBD	TBD	O	O	TBD	TBD	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	TBD	TBD	O	O	TBD	TBD	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	TBD	TBD	O	O	TBD	TBD	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→A	(→F)	O	O	TBD	TBD	O	O	TBD	TBD	O	O
G	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
H	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
I	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	TBD	TBD	(→I)	O	TBD	TBD	O	O
J	Wait-to-Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	TBD	TBD	→B	(→J)	TBD	TBD	N/A	O
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
L	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or lower priority.
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
[a] If SF is reasserted. [b] If SF-P is reasserted.

Table A.3 – State transition by Local Requests (1+1, unidirectional, revertive mode)

State		Local request													
		a	b	c	d	e	f	g	h	i	j	k	l	m	n
		Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	SD on working	Working recovers from SD	SD on protection	Protection recovers from SD	Manual switch	Clear	Exercise	WTR timer expired
A	No Request Working/Active Protection/Standby	→B	→C	→D[a)]	N/A	→E	N/A	TBD	TBD	TBD	TBD	→H	O	TBD	N/A
B	Lockout Working/Active Protection/Standby	O	O	O	O	O	O	TBD	TBD	TBD	TBD	O	→A or →D[b)] →E[c)]	TBD	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	TBD	TBD	TBD	TBD	O	→A or →D[c)]	TBD	N/A
D	Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→I	→E	N/A	TBD	TBD	TBD	TBD	O	O	TBD	N/A
E	Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	TBD	TBD	TBD	TBD	O	O	TBD	N/A
F	Signal Degrade (W) Working/Standby Protection/Active	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
G	Signal Degrade (P) Working/Active Protection/Standby	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
H	Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	TBD	TBD	TBD	TBD	O	→A	TBD	N/A
I	Wait-to-Restore Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	TBD	TBD	TBD	TBD	→H	→A	TBD	→A

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or lower priority.

[a)] It transits to the state D if the Signal Fail still exists after hold-off timer expires. [b)] If SF is reasserted. [c)] If SF-P is reasserted.

Table A.4 – State transition by Local Requests (1+1, unidirectional, non-revertive mode)

State	Local request												
	a	b	c	d	e	f	g	h	i	j	k	l	m
	Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	SD on working	Working recovers from SD	SD on protection	Protection recovers from SD	Manual switch	Clear	Exercise
A No Request Working/Active Protection/Standby	→B	→C	→D[a)]	N/A	→E	N/A	TBD	TBD	TBD	TBD	→H	O	TBD
B Lockout Working/Active Protection/Standby	O	O	O	O	O	O	TBD	TBD	TBD	TBD	O	→A or →D[b)] →E[c)]	TBD
C Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	TBD	TBD	TBD	TBD	O	→I or →D[b)]	TBD
D Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→I	→E	N/A	TBD	TBD	TBD	TBD	O	O	TBD
E Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	TBD	TBD	TBD	TBD	O	O	TBD
F Signal Degrade (W) Working/Standby Protection/Active	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
G Signal Degrade (P) Working/Active Protection/Standby	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
H Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	TBD	TBD	TBD	TBD	O	→I	TBD
I Do Not Revert Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	TBD	TBD	TBD	TBD	→H	O	TBD

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or lower priority.

[a)] It transits to the state D if the Signal Fail still exists after hold-off timer expires. [b)] If SF is reasserted. [c)] If SF-P is reasserted.

Appendix I

Selector types

…

Appendix II

Operation example of 1-phase APS protocol

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

II.1 Introduction

Operation examples of 1-phase APS protocol (1:1, revertive and non-revertive modes) are shown in Appendix I of ITU-T Rec. G.8031/Y.1342. These examples are protocol independent and apply to T-MPLS linear protection switching as well.

Bibliography

…

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, 2008