INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.1720

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(04/2003)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

Internet protocol aspects – Operation, administration and maintenance

Protection switching for MPLS networks

ITU-T Recommendation Y.1720

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

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

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

ITU-T Recommendation Y.1720

Protection switching for MPLS networks

Summary

This Recommendation provides requirements and mechanisms for 1+1 and 1:1 protection switching functionality for the user-plane in MPLS networks. The mechanism defined herein is designed to support end-to-end point-to-point LSPs. Protection switching functionality for multipoint-to-point and point-to-multipoint LSP are for further study. m:n protection switching is for further study. Hitless protection switching is outside the scope of this version of the Recommendation.

Source

ITU-T Recommendation Y.1720 was approved by ITU-T Study Group 13 (2001-2004) under the ITU-T Recommendation A.8 procedure on 6 April 2003.

Keywords

Defect, failure, LSP, MPLS, PML, PSL, protection switching, rerouting.

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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation Y.1720

Protection switching for MPLS networks

1 Scope

This Recommendation provides requirements and mechanisms for 1+1 and 1:1 protection switching functionality for the user-plane in MPLS networks. The mechanism defined herein is designed to support end-to-end point-to-point LSPs. Protection switching functionality for multipoint-to-point and point-to-multipoint LSP are for further study. m:n protection switching is for further study. 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 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.

[1] ITU-T Recommendation Y.1710 (2002), *Requirements for Operation & Maintenance functionality for MPLS networks*.

[2] ITU-T Recommendation Y.1711 (2002), *Operation & Maintenance mechanism for MPLS networks*.

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

NOTE – There is a limitation of the applicability of the architecture specified by ITU-T Rec. G.805. It is not applicable to LDP-based multipoint-to-point LSP and the case where PHP is in effect with the egress not supporting MPLS data plane.

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

[5] ITU-T Recommendation I.630 (1999), *ATM protection switching*.

[6] ITU-T Recommendation M.20 (1992), *Maintenance philosophy for telecommunication networks*.

[7] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[8] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

3 Definitions

This Recommendation defines the following terms:

3.1 1+1 protection: A protection mechanism in which the traffic is duplicated on the protection path (constantly bridged). The Path Merging LSR performs the switching of the traffic between the working and protection path.

3.2 1:1 protection: A protection mechanism in which the traffic is sent only on the working path or the protection path. The Path Switching LSR performs the switching of the traffic between the working and protection path.

3.3 bidirectional protection switching: A protection switching architecture in which, for a unidirectional failure, both directions of the LSP, including the affected direction and the unaffected direction, are switched to protection.

3.4 bridge: The action or function of transmitting identical traffic on both the working and protection LSP.

3.5 defect: (see Note 1) Interruption of the capability of an LSP to transfer user or OAM information.

3.6 extra traffic: Traffic that is purposely placed on the same network layer resource as a protection LSP (but in a separate LSP which is parallel to protection LSP) in the knowledge that on failure this (extra) traffic will be disconnected to make way for the protected traffic from the failed working connection.

3.7 failure: (see Note 1) Termination of the capability of an LSP to transfer user or OAM information. A failure can be caused by a persisting defect.

3.8 forced switch for working LSP: A switch action initiated by an operator command. Switch action is conducted unless a higher priority switch request (i.e., LoP) is in effect.

3.9 hold-off time: The time between declaration of signal degrade or signal fail, and the initialization of the protection switching algorithm.

3.10 manual switch: A switch action initiated by an operator command. Switch action is conducted unless an equal or a higher priority switch request (i.e., LoP, FS, SF or MS) is in effect.

3.11 MPLS protection domain: The set of LSRs over which a working path and its corresponding protection path are routed.

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

3.13 no request: A state where no protection switching request exists.

3.14 path switch LSR: An LSR that is responsible for switching or replicating the traffic between the working LSP and the protection LSP.

3.15 path merge LSR: An LSR that is responsible for receiving the protection path traffic, and either merges the traffic back onto the working path, or, if it is itself the destination, passes the traffic on to the higher layer protocols.

3.16 protection LSP: The LSP within the protection domain from which working traffic is received at the sink of the protection domain where a working LSP has failed.

3.17 protection switching: A recovery mechanism in which the protection LSP or path segments are created prior to the detection of a fault on the working path. In other words, a protection mechanism in which the protection LSP is pre-calculated, its capacity is pre-assigned and the protection LSP is pre-established.

3.18 rerouting: A recovery mechanism in which the recovery path or path segments are created dynamically after the detection of a fault on the working path. In other words, a recovery mechanism in which the recovery path is not pre-established.

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

3.20 selector: A switch which selects to receive the traffic from the working LSP or the protection LSP at the sink of the protection domain, or a switch which selects to send the traffic to the working LSP or the protection LSP at the source of the protection domain.

3.21 source of the protection domain: A transmitting endpoint (ingress) in a path switch LSR of the protection domain.

3.22 sink of the protection domain: A receiving endpoint (egress) in a path merge LSR of the protection domain.

3.23 transport entity: An architectural component which transfers information between its inputs and outputs within a layer network (see Note 2). An LSP is used as a transport entity in an MPLS network.

3.24 unidirectional protection switching: A protection switching architecture in which, for a unidirectional failure (i.e., a failure affecting only one direction of transmission), only the affected direction of the LSP is switched to protection.

3.25 wait to restore: An automatically initiated command that is issued when the working LSP exits SF condition. It is used to maintain the state until the Wait to Restore timer expires unless it is pre-empted by a higher priority bridge request.

3.26 wait to restore timer: A configurable timer which is used to delay before reversion.

3.27 working LSP: The LSP within the protection domain from which working traffic is received at the sink of the protection domain under fault-free condition in revertive mode.

NOTE 1 – ITU-T Rec. M.20 gives a more general and detailed definition.

NOTE 2 – ITU-T Rec. G.805 gives a more general and detailed definition.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

APS	Automatic Protection Switching
BDI	Backward Defect Indication
CV Packet	Connectivity Verification Packet
FDI	Forward Defect Indication
FS	Forced Switch
LDP	Label Distribution Protocol
LOCV	Loss of Connectivity Verification
LoP	Lockout of Protection
LSP	Label Switched Path
LSR	Label Switch Router
MPLS	Multi-protocol Label Switching
MS	Manual Switch
OAM	Operation, Administration and Maintenance
PHP	Penultimate Hop Popping
PML	Path Merge LSR
PS	Protection Switching
PSL	Path Switch LSR
SDH	Synchronous Digital Hierarchy
SF	Signal Fail

SLA Service Level Agreement

TTSI Trail Termination Source Identifier

5 Requirements

Techniques to enhance reliability performance of a network by providing a capability to recover from service interruption (e.g., due to defects) are referred to as survivability techniques. Survivability techniques include protection switching and rerouting. This Recommendation is developed to specify protection switching techniques. In this Recommendation the difference between protection switching and rerouting is intended to mean the following:

- Protection switching: This implies that both routing and resources are pre-calculated and allocated to a dedicated protection LSP prior to failure. Protection-switching therefore offers a strong assurance of being able to re-obtain the required network resources post-failure.
- Rerouting: This implies that a dedicated protection LSP is not defined, and so neither routing nor resources are pre-calculated/allocated prior to failure. Rerouting is commonly used to refer to cases where there are routing and signalling functions in operation, and that when a "re-connection request" has to be instigated on failure (either by the network, or by the customer), that this "reconnect request" has to contend with other similar traffic types for obtaining the required resource. Rerouting therefore offers no assurance of being able to re-obtain the required network resources post-failure and is generally slower than protection switching.

Protection switching is necessary for fast recovery from failure, and thereby enhances the reliability and availability performance of MPLS networks. For protection switching, the following features are required:

1) Protection switching should be applied to an entire LSP.
2) Prioritized protection between SF (Signal Fail) and operator switch requests (see Table 1).
3) The possibility to achieve protection at the MPLS layer as fast as possible (subject to the temporal resolution of the defect detection mechanism) should be provided.
4) Protection ratio of 100%, i.e., 100% of impaired working traffic is protected for a failure on a single working LSP.
5) An extra traffic capability should be supported when possible.

6 Principles

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 LSP is reserved for a selected working LSP. To be effective under all possible failures of the working LSP however, the protection LSP 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 LSP not to follow its shortest path.

The MPLS PS architecture can be a 1+1 type or a 1:1 type. Other types are for further study.

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

In the 1:1 architecture type, a protection LSP is dedicated to each working LSP. The working traffic is transmitted either by working or protection LSP. The method for a selection between the working

and protection LSPs depends on the mechanism. The protection LSP can be used to carry "extra traffic" when it is not used to transmit the working traffic.

The following list provides principles for MPLS protection architectures and mechanisms development.

1) Defects in layers above MPLS should not cause server layer protection switching. E.g., in case of ATM over MPLS, defects in ATM layer should not cause MPLS protection switching.

2) In general, if lower layer (e.g., SDH or optical) protection mechanisms are being utilized in conjunction with MPLS layer protection mechanisms, then the lower layers should have a chance to restore working traffic before the MPLS layer initiates protection actions (e.g., using a hold-off timer). The objective here is to avoid duplicated protection switching in different layer networks.

3) Protection switching actions in one protection domain should not adversely affect network operations, performance and protection switching in other domains.

4) The protection switching mechanism should facilitate fast recovery of working traffic to minimize the network outage, and ideally recovery should be before the unavailability entry threshold is reached.

7 Mechanisms

This clause describes mechanisms of unidirectional and bidirectional protection switching.

7.1 Unidirectional protection switching

7.1.1 Application architectures

7.1.1.1 Application architecture of unidirectional 1+1 protection switching

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

For example, if a unidirectional defect (in the direction of transmission from PSL to PML) occurs for the working LSP as in Figure 2, this defect will be detected at the sink of the protection domain at PML and the selector at PML will switch to the protection LSP.

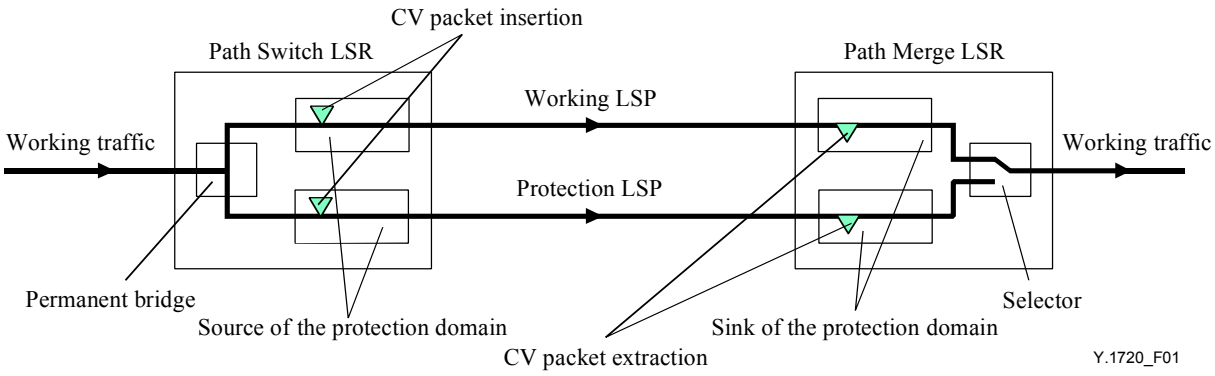

Figure 1/Y.1720 – Unidirectional 1+1 protection switching architecture

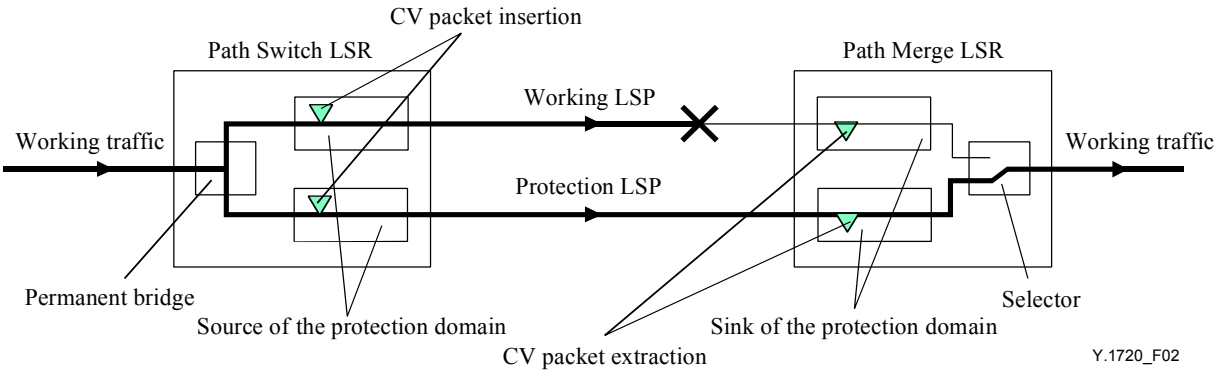

Figure 2/Y.1720 – Unidirectional 1+1 protection switching architecture – working LSP fails

7.1.1.2 Application architecture of unidirectional 1:1 protection switching

The 1:1 linear protection switching architecture is as shown in Figure 3. In the case of unidirectional protection switching operation as described here, protection switching is performed by the selector at the source of the protection domain based on purely local (i.e., at protection source) information. The working and protection traffic is permanently merged at the sink of the protection domain.

If CV packets or other continuity probe packets are used to detect defects of working or protection LSP, they are inserted at the source of the protection domain of both working and protection side and detected and extracted at the sink of the protection domain. It is noted that they should be sent regardless of whether the LSP is selected by the selector or not.

For example, if a unidirectional defect (in the direction of transmission from PSL to PML) occurs for the working LSP as in Figure 4, this defect is detected at the sink of the protection domain at PML and then reported by BDI to the source of the protection domain at PSL. The selector at PSL switches to the protection LSP on reception of this report.

NOTE – dTTSI_Mismerge cannot be protected by 1:1 protection switching.

When SF for working LSP is declared and user traffic is transmitted by protection LSP, FDI packet and user traffic may be merged at the sink of the protection domain. Nodes in downstream may receive FDI packets, CV packets and user traffic at the same time. Same applies to the case where SF for protection LSP is declared. One way to solve this problem is to use a merging selector. The operation of the merging selector under a defect being on the working LSP is the following:

1) Receive FDI packets or detect a lower layer defect at the egress of the working LSP.
2) Switch the merging selector at the egress (i.e., open the switch on working LSP and close the switch on protection LSP).
3) Send BDI packets on working LSP.
4) Switch the selector at the ingress (i.e., working LSP to protection LSP and cut off the extra traffic).

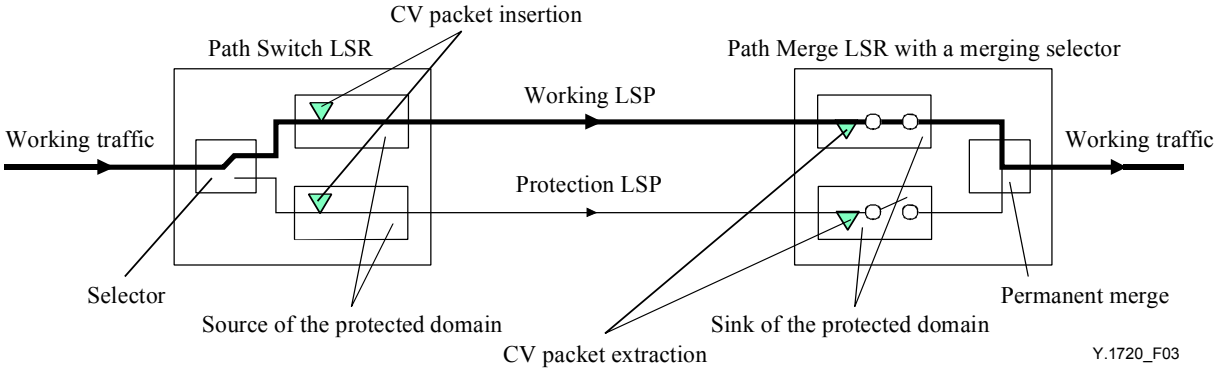

Figure 3/Y.1720 – Unidirectional 1:1 protection switching architecture

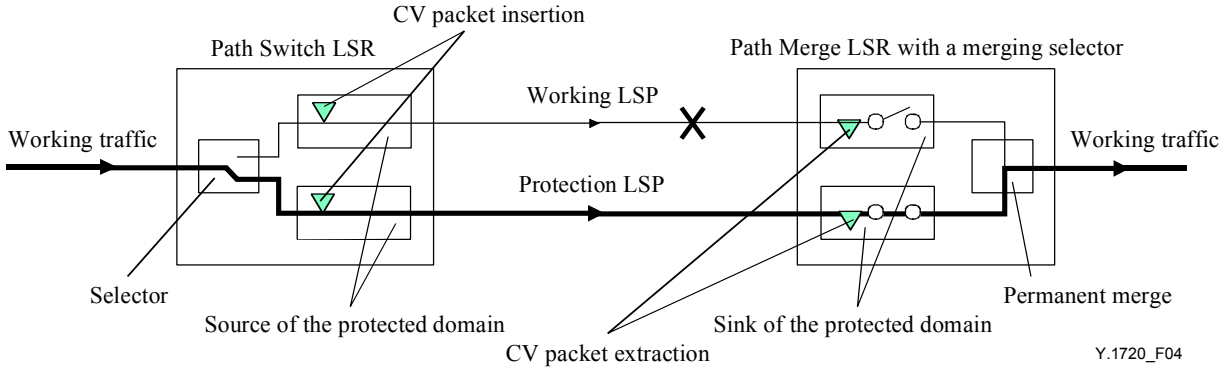

Figure 4/Y.1720 – Unidirectional 1:1 protection switching architecture – working LSP fails

7.1.1.3 Extra traffic

The 1:1 architecture can support extra traffic. As the traffic from the working and the protection LSPs is merged at the sink point of the protection domain, extra traffic must be transported via a separate LSP for which the physical route is the same as the protection LSP (see Figure 5) in order to avoid the extra traffic and the working traffic being merged and to share the bandwidth between them. When the working traffic is switched over to the protection LSP, the extra traffic is disconnected to make way for the protected traffic from the failed working connection (see Figure 6). This generally requires a protection switching coordination protocol. In this Recommendation, BDI is used as the 1-phase protocol (see also ITU-T Rec. I.630). Connectivity verification of an extra traffic LSP is optional. In case notification of disconnection of extra traffic is required, connectivity verification should be used.

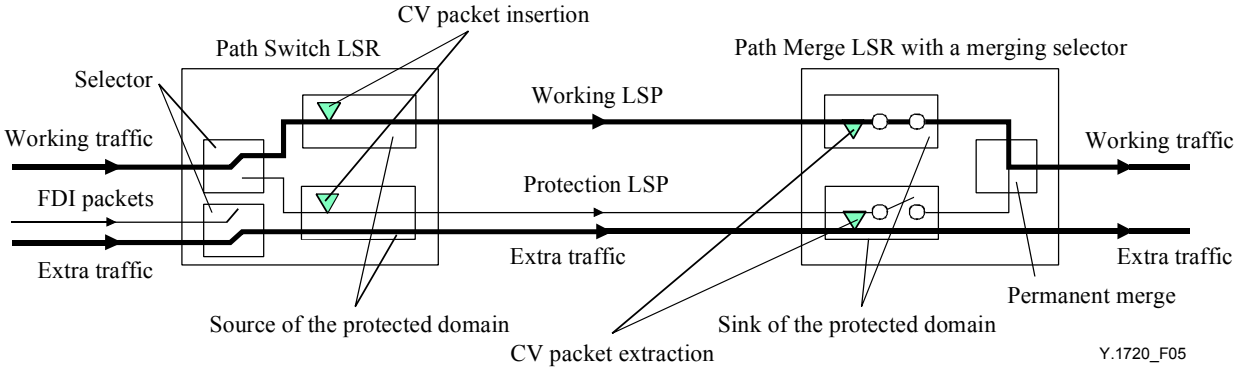

Figure 5/Y.1720 – 1:1 architecture with extra traffic

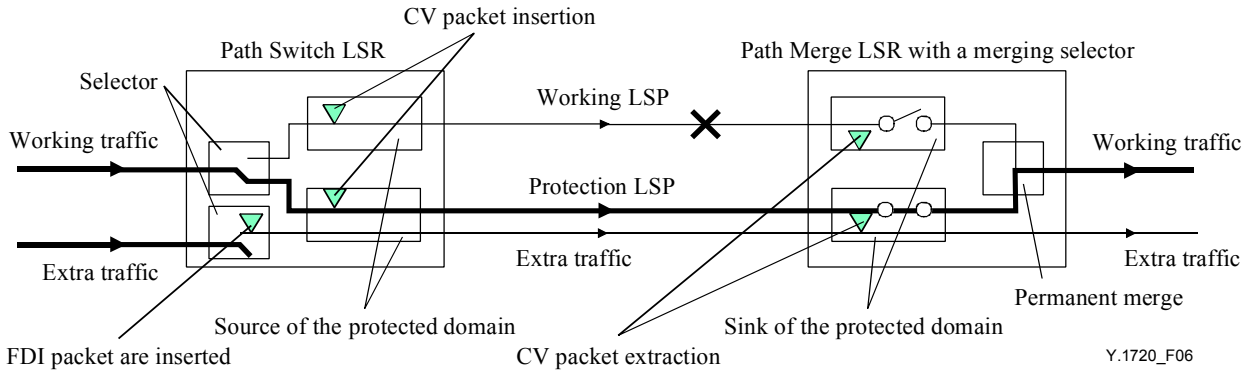

Figure 6/Y.1720 – 1:1 architecture with extra traffic – working LSP fails

7.1.2 Protection switching trigger mechanism

Protection switching action should 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 is declared on the connected LSP (i.e., working LSP or protection LSP) and is not declared on the other LSP and the hold-off timer has expired; or
3) the wait to restore timer expires (revertive mode) and SF is not declared on the working LSP.

7.1.2.1 Manual control

Manual control of the protection switching function may be transferred from the operation system.

7.1.2.2 Signal Fail declaration conditions

7.1.2.2.1 1+1 architecture

For 1+1 architecture, Signal Fail (SF) is declared when the sink point of the protection domain enters the LSP Trail sink Near-End Defect State by entering the dServer, dLOCV, dTTSI_Mismatch, dTTSI_Mismerge, dExcess, or dUnknown condition.

In order to achieve fast protection (the requirement for fast protection is under study) SF can be declared when an FDI packet is received by the sink of the protection domain before it enters other defect conditions (e.g., dLOCV). It allows fast protection against the defects sourced from layers below the MPLS layer (and this requires that the incoming FDI have the DT codepoint 0x0101).

NOTE – It is only appropriate to be used if the lower layer is not protected. If the lower layer is also protected it may lead to unnecessary protection switching by declaring SF on reception of FDI packets.

In the case where the CV function is not activated, SF is declared when an FDI packet is received by the sink of the protection domain. It only applies to the defects sourced from layers below the MPLS layer (and this requires that the incoming FDI have the DT codepoint 0x0101).

7.1.2.2.2 1:1 architecture

For 1:1 architecture, Signal Fail (SF) is declared when:

- the source of the protection domain enters the Trail sink Far-End Defect State by receiving a BDI packet (from the return LSP or out of band).

NOTE – Protection against bidirectional LSP defect is for further study.

7.1.3 Compliance with network objectives

The following network objectives apply:

1) *Operating modes*

   Revertive and non-revertive switching are provided.

2) *Manual control*

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

3) *Other switch initiation criteria*

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

7.1.4 Switch initiation criteria

The following switch initiation criteria exist:

1) an externally initiated command (Clear, Lockout of Protection, Forced Switch, Manual Switch);
2) an automatically initiated command (Signal Fail) associated with a protection domain; or
3) a state (Wait to Restore, No Request) of the protection switching function.

All requests are local (i.e., protection sink for 1+1 architecture and protection source for 1:1 architecture). The priority of local requests is given in Table 1.

Table 1/Y.1720 – Priority of local requests

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

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

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

7.1.4.1 Externally initiated commands

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

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

Lockout of Protection (LoP): Fix the selector position on the working LSP. Prevents the selector from switching to the protection LSP when it is selecting the working LSP. Switches the selector from the protection to the working LSP when it is selecting the protection LSP.

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

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

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

7.1.4.2 FDI triggered protection switch

In the case of FDI triggered protection switching, if the LSP with SF never enters a near end defect state, there may be a need to prevent frequent transitions. If so, some time may be defined that must pass before taking another protection switching action. This is for further study.

7.1.4.3 States

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

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

7.1.5 Protection switching protocol

In the unidirectional 1+1, and 1:1 protection switching architecture, there is no need for APS protocol.

7.1.6 Unidirectional protection switching algorithm operation

7.1.6.1 Control of the selector

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

7.1.6.2 Revertive mode

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

7.1.6.3 Non-revertive mode

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

7.2 Mechanisms of bidirectional protection switching

For further study.

Appendix I

Bibliography

– IETF RFC 3469 (2003), *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2003