

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1720

(12/2006)

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

Internet protocol aspects – Operation, administration and
maintenance

Protection switching for MPLS networks

ITU-T Recommendation Y.1720



International
Telecommunication
Union

Documents
Document Sharing Hub

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.

ITU-T Recommendation Y.1720

Protection switching for MPLS networks

Summary

ITU-T Recommendation Y.1720 provides requirements and mechanisms for 1+1, 1:1, shared mesh, and packet 1+1 protection switching functionality for the user-plane in MPLS layer 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 on 14 December 2006 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

LSP, MPLS, PML, protection switching, PSL, re-routing.

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 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 2007

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Definitions defined elsewhere	2
3.2	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	3
5	Requirements	4
6	Principles	5
7	Mechanisms	6
7.1	Unidirectional protection switching	6
7.2	Mechanisms of bidirectional protection switching.....	15
8	Security aspects	15
Appendix I – Example of protection capacity sharing for shared mesh protection switching.....		16
Appendix II – Packet 1+1 example realization.....		18
II.1	Dual-feed and select mechanism	19
II.2	Analysis of the packet 1+1 scheme	19
Bibliography.....		27

ITU-T Recommendation Y.1720

Protection switching for MPLS networks

1 Scope

This Recommendation provides requirements and mechanisms for 1+1, 1:1, shared mesh, and packet 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 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*.

NOTE – There is a limitation of the applicability of the architecture specified by [ITU-T 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.

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

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

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

[ITU-T M.495] ITU-T Recommendation M.495 (1988), *Transmission restoration and transmission route diversity: Terminology and general principles*.

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

[ITU-T Y.1711] ITU-T Recommendation Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks*.

[IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*. Category: Standards Track.

[IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*. Category: Standards Track.

3 Definitions

3.1 Definitions defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 **bidirectional protection switching:** ITU-T Rec. G.780/Y.1351.
- 3.1.2 **unidirectional protection switching:** ITU-T Rec. G.780/Y.1351.
- 3.1.3 **signal fail (SF):** [ITU-T G.805].
- 3.1.4 **trail:** [ITU-T G.805].
- 3.1.5 **defect:** ITU-T Rec. G.806.
- 3.1.6 **failure:** ITU-T Rec. G.806].
- 3.1.7 **APS protocol:** ITU-T Rec. G.870/Y.1352.
- 3.1.8 **switch:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.1 **forced switch:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.2 **manual switch:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.3 **lockout of protection:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.4 **wait to restore:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.5 **clear:** ITU-T Rec. G.870/Y.1352.
- 3.1.8.6 **no request:** ITU-T Rec. G.870/Y.1352.
- 3.1.9 **component:** ITU-T Rec. G.870/Y.1352.
- 3.1.9.1 **protected domain:** ITU-T Rec. G.870/Y.1352.
- 3.1.9.2 **bridge:** ITU-T Rec. G.870/Y.1352.
- 3.1.9.3 **selector:** ITU-T Rec. G.870/Y.1352.
- 3.1.9.4 **sink node:** ITU-T Rec. G.870/Y.1352.
- 3.1.9.5 **source node:** ITU-T Rec. G.870/Y.1352.
- 3.1.10 **architecture:** ITU-T Rec. G.870/Y.1352.
- 3.1.10.1 **1+1 protection architecture:** ITU-T Rec. G.870/Y.1352.
- 3.1.10.2 **1:n protection architecture:** ITU-T Rec. G.870/Y.1352.
- 3.1.10.3 **non-revertive protection switching:** ITU-T Rec. G.870/Y.1352.
- 3.1.10.4 **revertive protection switching:** ITU-T Rec. G.870/Y.1352.
- 3.1.11 **signal:** ITU-T Rec. G.870/Y.1352.
- 3.1.11.1 **normal traffic:** ITU-T Rec. G.870/Y.1352.
- 3.1.11.2 **extra traffic signal:** ITU-T Rec. G.870/Y.1352.
- 3.1.12 **time:** ITU-T Rec. G.870/Y.1352.
- 3.1.12.1 **hold-off time:** ITU-T Rec. G.870/Y.1352.
- 3.1.12.2 **wait-to-restore time:** ITU-T Rec. G.870/Y.1352.
- 3.1.13 **transport entity:** ITU-T Rec. G.870/Y.1352.
- 3.1.13.1 **protection transport entity:** ITU-T Rec. G.870/Y.1352.

3.1.13.2 working transport entity: ITU-T Rec. G.870/Y.1352.

3.2 Terms defined in this Recommendation

This Recommendation uses the following terms:

3.2.1 shared mesh protection: Shared mesh protection switching can be viewed as an extension of 1:1 protection. It provides sharing of bandwidth between protection LSPs corresponding to working LSPs that belong to disjoint links, nodes, or SRGs.

3.2.2 shared risk group (SRG): SRG is a group of links or nodes that can fail simultaneously due to a single failure incident. For example, fibres within a conduit belong to an SRG, because a single conduit breakage can cut all fibres passing through it.

3.2.3 packet 1+1 protection: Like 1+1 protection the traffic is fed onto both LSPs. Packet level 1+1 allows selection of incoming packet from any of the two LSPs irrespective of the LSP from which the last packet was selected. That is, packet 1+1 protection treats both LSPs as working as opposed to designating one LSP as working while the other as the protection LSP.

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

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

3.2.6 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.

3.2.7 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.

3.2.8 re-routing: 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.

3.2.9 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 – [ITU-T M.20] and [ITU-T G.805] give a more general and detailed definition.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APS	Automatic Protection Switching
BDI	Backward Defect Indication
CV Packet	Connectivity Verification Packet
FDI	Forward Defect Indication
FFD Packet	Fast Failure Detection Packet
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	Multiprotocol 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 re-routing. This Recommendation is developed to specify protection switching techniques. In this Recommendation, the difference between protection switching and re-routing 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.
- Re-routing: This implies that a dedicated protection LSP is not defined, and so neither routing nor resources are pre-calculated/allocated prior to failure. Re-routing 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. Re-routing, 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 signal fail (SF) 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, a 1:1 type, a shared mesh type, or a packet 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.

NOTE 1 – To avoid a single point of failure, the working LSP and the protection LSP shall be routed along disjoint paths.

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.

NOTE 2 – To avoid a single point of failure, the working LSP and the protection LSP shall be routed along disjoint paths.

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.

In the shared mesh architecture type, possible sharing of protection capacity between disjoint link, node, or SRG failures in the network is achieved while guaranteeing recovery from a single failure. For each link in the network, it keeps track of all the working paths whose traffic will be switched onto it after a given failure. By keeping track of this, it only needs to reserve the maximum of the protection capacity required to protect a single failure in the network.

In the packet 1+1 architecture type, the traffic is transmitted simultaneously onto two possibly disjoint routed LSPs to the sink of the protection domain. Each pair of duplicate transmitted packets is assigned the same identifier (sequence number) but distinct from the other pairs of duplicate packets. At the sink of the protection domain, packet level selection mechanism is employed to select one of the two possibly received copies of each packet. 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. For example, 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.