



uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES
ET POSTDOCTORALES



FACULTY OF GRADUATE AND
POSTDOCTORAL STUDIES

Khaled Maamoun

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A.Sc. (Electrical Engineering)

GRADE / DEGREE

School of Information Technology and Engineering

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Survivable IP Over Optical Transport Networks

TITRE DE LA THÈSE / TITLE OF THESIS

H. Mouftah

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

A. Matrawy

S. Shirmohammadi

Gary W. Slater

Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

Survivable IP over Optical Transport Networks

Khaled Maamoun

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the MASc degree in
Electrical and Computer Engineering

School of Information Technology and Engineering
Faculty of Engineering
University of Ottawa

©Khaled Maamoun, Ottawa, Canada, 2007



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 978-0-494-32468-4

Our file Notre référence

ISBN: 978-0-494-32468-4

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

Abstract

Survivability strategies for a single network layer have been investigated for many years in the research and development of communication networks. Some of these networks already have available standards for protection methods and techniques (e.g. SONET). However, using only one survivability technique running in a single-layer is not always the optimal solution if we want to achieve a certain level of QoS for all services without increasing the cost of their use. One of the most promising solutions for overcoming this problem is to use multi-layer survivability techniques running in different network layers. The use of multi-layer survivability strategies requires precise definitions of the survivability functionalities that need to be allocated at each layer and the coordination between the network layers.

This thesis investigates survivability schemes for optical networks that rely only on a single layer, as well as for those that have more than one layer survivability functions and uses different approaches to solve QoS survivability related problems. We have simulated the restoration process of single transport layer: IP; ATM; SONET and OTN, which have been analyzed by similar studies. Also, we have simulated the process of the multi-layer restoration schemes for previously analyzed IP/SONET , IP/OTN and IP-MPLS/OTN by using the hold-off timer concept. We have extended their restoration concept and applied it for IP/OTN and ATM/SONET

restoration schemes. Further more, we have introduced IP Restoration/OTN Protection combined multi-layer survivability, IP Restoration/SONET Protection combined multi-layer survivability and IP-MPLS Protection and Restoration/OTN Protection combined multi-layer survivability. In this thesis, we have combined the analyses with simulations to form a comprehensive study for the IP over OTN survivability across different architectures. The study focuses on four of the most commonly used network architectures of the IP over OTN architecture possibilities: IP/POS/OTN; IP/GbE/OTN; IP-MPLS/OTN, and the traditional, still commonly used IP/ATM/SONET/OTN.

Acknowledgements

First, I would like to express my sincere gratitude to my supervisor, Professor Hussein T. Mouftah, for his outstanding guidance and support through my graduate studies. It has been a great privilege for me to be able to learn from his expertise in academic research. He has always shared his insightful entrepreneurial experiences and his perspectives on the telecommunications network industry. His constant emphasis on practical contributions has helped to shape the direction of my research which has resulted in this thesis.

In addition, I am also grateful for the support of my family and my beloved daughter Maryam, who has always believed in me. Their constant encouragement and reassurance have given me the strength to complete my graduate studies.

Contents

Abstract.....	ii
Acknowledgements	iv
Contents	v
List of Figures.....	ix
List of Tables	xiii
List of Acronyms	xv
Chapter 1: Introduction.....	1
1.1. Background	1
1.1.1. Layering Architecture Possibilities.....	2
1.1.2. Network Survivability Schemes.....	3
1.1.2.1. Protection	3
1.1.2.2. Restoration	3
1.1.3. Multi-layer Survivability Ideology	4
1.2. Motivation.....	5
1.3. Objective	6
1.4. Contributions.....	7
1.5. Thesis Organization	8
Chapter 2: Survivability in Network Transport Layers	10
2.1. Survivability in the Optical Layer.....	10
2.1.1. Protection in the Optical Layer	11
2.1.1.1. OMS Protection	11
2.1.1.2. OCh Protection.....	12
2.1.1.3. Dedicated and Shared Protection	14
2.1.1.3.1 Dedicated Protection	14
2.1.1.3.2 Shared Protection	15
2.1.1.4. Link and Path Protection.....	16
2.1.2. Restoration in the Optical Layer	17
2.1.2.1. Centralized and Distributed Restoration Control Architectures ..	17
2.1.2.2. Dynamic and Pre-planned Restoration Control Architectures....	18
2.1.2.3. Adjacent-node, Intermediate Node and End-to-end Restoration	
Types	18
2.2. Survivability in the IP Layer.....	19
2.2.1. IP Protection.....	19

2.2.2.	IP Restoration.....	20
2.3.	Survivability in SONETs	21
2.3.1.	SONET Protection with APS	21
2.3.2.	SONET Protection in the Self-Healing Rings.....	23
2.3.3.	SONET Restoration in DCS Self-Healing Mesh Networks	26
2.3.4.	Relative Comparisons among the SONET APS/DP, SHR, and Self-healing Networks (SHN).....	26
2.4.	Survivability in ATM.....	27
2.4.5.	ATM Protection	28
2.4.6.	ATM Restoration	31
2.4.6.1.	Two-step Restoration Scheme	31
2.4.7.	Survivability Quality of Service	33
2.5.	Survivability in the MPLS (GMPLS)	34
2.5.8.	MPLS Protection.....	34
2.5.9.	MPLS Restoration.....	35
2.5.9.1.	Failure Notification.....	36
2.5.9.2.	Restoration Time.....	36
2.5.10.	MPLS Restoration Practice.....	36
Chapter 3:	Multi-layer Survivability Solutions	38
3.1.	Survivability Strategies.....	40
3.1.1.	Appropriate Selection of Survivability Schemes	40
3.1.2.	Hold-off Time	41
3.1.3.	Inter-layer Signaling	42
3.1.4.	Layer Escalation.....	43
3.1.5.	Sub-network Escalation	44
3.1.6.	Scheme Escalation	44
3.1.7.	Management Integration	44
3.2.	Survivability in Different Integrated Multi-layer Network Architectures	45
3.3.	The IP/ATM/SONET/OTN Architecture.....	45
3.3.8.	Available Single-layer Survivability Schemes	47
3.3.9.	Available Multi-layer Survivability	48
3.4.	The IP/SONET (POS)/OTN Architecture	49
3.4.1.	Available Single-layer Survivability Schemes	50
3.4.2.	Available Multi-layer Survivability	50
3.5.	The IP/GbE/OTN Architecture	51
3.5.1.	Available Single-layer Survivability Schemes	52
3.5.2.	Available Multi-layer Survivability	53
3.6.	IP-MPLS/OTN Architecture	54
3.6.1.	Available Single-layer Survivability Schemes	54
3.6.2.	Available Multi-layer Survivability	55
Chapter 4:	Performance Evaluation.....	56
4.1.	Network Architecture Model used.....	56
4.1.1.	Network Traffic.....	57
4.1.1.1.	Network Traffic Process	57
4.1.2.	Routing and Wavelength Assignment RWA	58

4.1.3.	Wavelength Converters.....	58
4.1.4.	Load Balancing	59
4.1.5.	Network Management.....	59
4.2.	System Parameters	59
4.3.	Simulated Survivability Schemes	61
4.3.1.	OTN Restoration	61
4.3.2.	SONET Restoration	61
4.3.3.	ATM Restoration	62
4.3.4.	IP Restoration.....	62
4.4.	Simulation Results	63
4.4.1.	Single-layer Survivability; IP Restoration	63
4.4.2.	Single-layer Survivability; ATM Restoration.....	65
4.4.3.	Single-layer Survivability; SONET Restoration.....	66
4.4.4.	Single-layer Survivability; OTN Restoration	68
4.4.5.	Multi-layer Survivability; ATM/SONET Restoration	69
4.4.6.	Multi-layer Survivability; IP/SONET Restoration	71
4.4.7.	Multi-layer Survivability; IP/OTN Restoration	72
4.4.8.	Multi-layer Survivability; IP-MPLS/OTN Restoration	74
4.4.9.	Combined Multi-layer Survivability; IP -Restoration/OTN Protection	75
4.4.10.	Combined Multi-layer Survivability; IP Restoration/SONET Protection	77
4.4.11.	Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/OTN-Protection	78
4.4.12.	Simulation Graphs Comparison	80
Chapter 5:	Conclusions.....	83
5.1.	Single-Layer Restoration Schemes	83
5.2.	Multi-Layer Restoration Schemes	85
5.3.	Combined Survivability Schemes.....	86
5.4.	Future Research	88
References		89
Appendix A:	Network Failures.....	106
A.1.	Failure Impact on the Service Layers	109
A.2.	Single-layer Network Survivability Measure	110
A.2.1.	Quality of Protection (QoP)	110
A.2.2.	Priority Classes	111
Appendix B:	Survivability Analysis in the Network Transport Layers	114
B.1.	Optical Layer	114
B.2.	IP Layer.....	119
B.2.1.	IP Layer (OSI layer 3) Routing Protocols.....	119
B.2.1.1.	Interior Gateway Protocols (IGP)	120
B.2.1.2.	Exterior Gateway Protocols (EGP)	121
B.3.	SONET.....	122
B.4.	ATM.....	127
B.4.1.	Survivable ATM Network Management Architecture.....	131

B.4.2.	Operation Administration and Maintenance (OAM) Cell	132
B.5.	MPLS (GMPLS)	135
B.5.1.	MPLS Principles	136
B.5.2.	Multi-Protocol Lambda Switching	137
B.5.3.	MPLS Routing Protocols	138
B.5.4.	MPLS Signaling Protocols.....	138
Appendix C: Encapsulation Methods for the Different Network Architectures		
		141
C.1.	IP/ATM/SONET/OTN Architecture.....	141
C.2.	IP/SONET (POS)/OTN Architecture.....	145
C.3.	IP/GbE/OTN Architecture	148
C.4.	IP-MPLS/OTN Architecture	149

List of Figures

Fig. 1.1: IP to OTN Choices [BON01]	2
Fig. 1.2: Comparison between Survivability Schemes for Different Network Layers	4
Fig. 2.1: Optical Layer Survivability Techniques [MAL02]	10
Fig. 2.2: Possible Node for OMSP in a Ring Configuration	11
Fig. 2.3: 1+1 OChP Ring	12
Fig. 2.4: SNCP (OChP) Node in a Ring Configuration	13
Fig. 2.5: Trail Protection (OChP) Node in a Ring Configuration	13
Fig. 2.6: Architecture of OADM for 1+1 OCh Protection: (a) SNCP and (b) Trail Protection	14
Fig. 2.7: Architecture of 1+1 Protection Schemes [ZHO00]	15
Fig. 2.8: Architecture of 1:1 Protection Schemes [ZHO00]	15
Fig. 2.9: Link-based Protection [ZHO00]	16
Fig. 2.10: Path-based Protection [ZHO00]	17
Fig. 2.11: Protection against Router Failures by Duplication	20
Fig. 2.12: SONET 1:N APS [ZHO00]	22
Fig. 2.13: SONET APS/DP (Dedicated Protection) 1+1 Protection of the Path AD [MAL02]	23
Fig. 2.14: SONET SHR [ZHO00]	24
Fig. 2.15: LTE with BSHR/4 in Normal Working Condition	24
Fig. 2.16: LTE with BSHR/4 with a Working Link in Failure	25
Fig. 2.17: LTE with BSHR/4 with Both Working and Protection Links in Failure	25
Fig. 2.18: ATM 1:1 APS Protection [KAW98C]	28
Fig. 2.19: ATM Self-healing Ring (SHR) [KAW98C]	29
Fig. 2.20: ATM Self-healing Network (SHN) [KAW98C]	30

Fig. 2.21: ATM Failure Resistance Virtual Path FRVP [KAW98C]	30
Fig. 2.22: ATM Two-steps Restoration Mechanism	32
Fig. 2.23: Restoration Schemes in IP-MPLS [ZHA02]	35
Fig. 2.24: Restoration Re-routing Process	37
Fig. 3.1: General Example of IP over ATM over SONET Encapsulation for Transport over a OTN Network	46
Fig. 3.2: Three Options for ATM in SONET [AND97B]	47
Fig. 3.3: Example of IP over SONET over OTN Network	49
Fig. 3.4: Example of IP being transported over a OTN Ring with Gigabit Ethernet Framing	52
Fig. 4.1: Network Architecture Model used in the Simulation	56
Fig. 4.2: Single-layer Survivability; IP Restoration	63
Fig. 4.3: Single-layer Survivability; IP Restoration (after recovery view)	64
Fig. 4.4: Single-layer Survivability; ATM Restoration (complete view)	65
Fig. 4.5: Single-layer Survivability; ATM Restoration (after recovery view)	66
Fig. 4.6: Single-layer Survivability; SONET Restoration (complete view)	66
Fig. 4.7: Single-layer Survivability; SONET Restoration (after recovery view)	67
Fig. 4.8: Single-layer Survivability; OTN Restoration (complete view)	68
Fig. 4.9: Single-layer Survivability; OTN Restoration (after recovery view)	68
Fig. 4.10: Multi-layer Survivability; ATM/SONET Restoration (complete view)	69
Fig. 4.11: Multi-layer Survivability; ATM/SONET Restoration (after recovery view)	70
Fig. 4.12: Multi-layer Survivability; IP/SONET Restoration (complete view)	71
Fig. 4.13: Multi-layer Survivability; IP/SONET Restoration (after recovery view)	71
Fig. 4.14: Multi-layer Survivability; IP/OTN Restoration (complete view) ...	72
Fig. 4.15: Multi-layer Survivability; IP/OTN Restoration (after recovery view)	73
Fig. 4.16: Multi-layer Survivability; MPLS/OTN Restoration (complete view)	74
Fig. 4.17: Multi-layer Survivability; MPLS/OTN Restoration (post recovery view)	74

Fig. 4.18: Combined Multi-layer Survivability; IP Restoration/OTN Protection.....	75
Fig. 4.19: Combined Multi-layer Survivability; IP Restoration/OTN Protection (post recovery view)	76
Fig. 4.20: Combined Multi-layer Survivability; IP Restoration/SONET Protection.....	77
Fig. 4.21: Combined Multi-layer Survivability; IP Restoration/SONET Protection (post recovery view)	78
Fig. 4.22: Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/SONET-Protection.....	79
Fig. 4.23: Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/SONET-Protection (post recovery view).....	80
Fig. 4.24: Single layer Survivability (after recovery view).....	81
Fig. 4.25: Multi-layer Survivability (after recovery view).....	81
Fig. 4.26: Combined Multi-layer Survivability (after recovery view)	82
Fig. A.1: Causes of Network Failure [LAB99]	107
Fig. A.2: Impact of Restoration Time on some IP-based Services.....	110
Fig. B.1: Optical Sub-layers	114
Fig. B.2: Optical Sub-layers [ITU03A]	115
Fig. B.3: Optical Channel OCh [ITU03A]	116
Fig. B.4: OTU Transmission [ITU03A]	116
Fig. B.5: SONET Sub-layers	123
Fig. B.6: SONET Layer Model [NAT03].....	123
Fig. B.7: STS-1 Frame Structure	124
Fig. B.8: STS-1 TOH & POH.....	124
Fig. B.9: ATM Protocol Architecture [STA02]	127
Fig. B.10: ATM Cell Format [STA02].....	129
Fig. B.11: ATM Connection and Connection Segment Hierarchy [AND97B]	129
Fig. B.12: Call Establishment Using Virtual Paths [STA02]	130
Fig. B.13: ATM Terminal Messages Exchange	131
Fig. B.14: ATM Survivable ATM Network Management Architecture [MUR97]	132
Fig. B.15: ATM OAM Fault Management Cell with Defect Type Indicator [AND97B]	134
Fig. B.16: Alarm Transmission Mechanism for VP Layer [KAW98C].....	135

Fig. B.17: MPLS in Action: Simple Label-swapping and Forwarding in the Core	136
Fig. B.18: Candidate OXC Systems Architecture	138
Fig. C.1: Adding LLC/SNAP Overhead to IP Datagram	143
Fig. C.2: AAL Type 5 [STA02]	143
Fig. C.3: Example of AAL 5 Transmissions [STA02]	144
Fig. C.4: ATM Cell Mapping into a STS-1	144
Fig. C.5: ATM Cell Mapping into a STS-3c	145
Fig. C.6: POS (Packet over SONET)	146
Fig. C.7: Gigabit Ethernet Frame	148
Fig. C.8: Gigabit Ethernet Sub-layers	149
Fig. C.9: An illustration of IP Packet that contains MPLS Header	150

List of Tables

Table 2.1: Comparison of Adjacent Node, Intermediate Node, and End-to-End Restoration Types	19
Table 2.2: Comparison between SHR Schemes	25
Table 2.3: Relative Comparisons between the SONET APS/DP, SHR, and DCS Self-healing Networks.....	27
Table 2.4: Comparison between ATM Protection and Restoration [KAW98C]	33
Table 3.1: Survivability Capabilities of the Network layers in the IP/ATM/SONET/OTN Architecture	47
Table 3.2: Available Multi-layer Survivability Schemes in the IP/ATM/SONET/OTN Architecture	48
Table 3.3: Survivability Capabilities of the Network layers in the IP/POS/OTN Architecture.....	50
Table 3.4: Available Multi-layer Survivability Schemes in the IP/SONET (POS)/OTN Architecture.....	51
Table 3.5: Survivability Capabilities of the Network Layers in the IP/GbE/OTN Architecture.....	53
Table 3.6: Available Multi-layer Survivability Schemes in the IP/GbE/OTN Architecture	53
Table 3.7: Survivability Capabilities of the Network Layers in the IP-MPLS/OTN Architecture	55
Table 3.8: Available Multi-layer Survivability Schemes in the IP-MPLS/OTN Architecture	55
Table 4.1: Simulation Network Parameters.....	60
Table 5.1: Selected Single Layer Survivability for the Four Network Architectures	85
Table 5.2: Selected Multi-layer Survivability Schemes for the four Network Architectures	86
Table 5.3: Proposed Multi-layer Combined Survivability Schemes for the Four Network Architectures	88

Table A.1: List of Failure Types and Possible Causes [LAB99]	106
Table A.2: Classification of Failures	108
Table A.3: Impact of Restoration Time on Services [KAW98C]	109
Table B.1: Optical Sub-layers [MAL02]	115
Table B.2: TCM Status Interpretation [ITU03A]	117
Table B.3: PM Status Interpretation [ITU03A]	117
Table B.4: Fault Indication Codes Interpretation [ITU03A]	118
Table B.5: Payload Type Code Points [ITU03A]	118
Table B.6: Optical Sub-layers and its SONET Equivalents	119
Table B.7: A Comparison between Distance-vector and Link-state Routing Algorithms [BLA00]	121
Table B.8: A Comparison between Border Gateway Protocol BGP and Inter- Domain Routing Protocol IDRP	122
Table B.9: STS-1 Header Information	125
Table B.10: SONET K1 & K2 Messages	125
Table B.11: Summarization the ATM Layers Functions	127
Table B.12: Summary of ITU-T 1.610 ATM-layer OAM Functionality [AND97B]	133
Table C.1: Protocol Stack for Classical IP over ATM over SONET	142
Table C.2: Protocols used for IP over SONET	145

List of Acronyms

ADM	Add-Drop Multiplexer
AIS	Alarm Indication Signal
APS	Automatic Protection Switching
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BGP	Border Gateway Protocol
CoS	Class of Services
DPT	Dynamic Packet Transport
EGP	Exterior Gateway Protocol
FAS	Frame Alignment Signal
FEC	Forwarding Equivalence Class
FIS	Failure Indication Signal
GbE	Gigabit Ethernet
HDLC	High-level Data Link Control
IGP	Interior Gateway Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intelligent Protection System
ITU	International Telecommunication Union
LAN	Local Area Network
L2	Layer 2

L3	Layer 3
LF	Link Failure
LLC	Logical Link Control
LOP	Loss Of Packet
LOS	Loss Of Signal
LSP	Lable Switched Path
LSR	Lable Switch Router
MAC	Medium Access Control
MPLS	Multi Protocol Label Switching
MP λ S	Multi Protocol Lambda Switching
MSP	Multiplex Section Protection
NE	Network Element
OAM	Operation, Administration and Maintenance
OADM	Optical Add-Drop Multiplexer
OCh	Optical Channel
OEXC	Opto-Electric Cross-Connect
OMS	Optical Multiplex Section
OMSP	Optical Multiplex Section Protection
OSC	Optical Supervisory Channel
OSPF	Open Shortest Path First
OTN	Optical Transport Network
OTS	Optical Transmission Section
OXC	Optical Cross-Connect
POS	Packet Over SONET/SDH
PPP	Point-to-Point Protocol
QoS	Quality of Service
RIP	Routing Information Protocol
SDH	Synchronous Digital Hierarchy
SNCP	Sub-Network Connection Protection

SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SRP	Spatial Reuse Protocol
STA	Spanning Tree Algorithm
STM	Synchronous Transport Module
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
TOS	Type Of Service
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing

Chapter 1: Introduction

1.1. Background

There is a focused interest on the development and use of optical network technologies in the Internet world due to their almost unlimited bandwidth, which has been a result of the exponential growth of Internet broadband services.

The tremendous traffic capacities of optical networks have been achieved by Wavelength Division Multiplexing (WDM), despite ongoing development in the control plane of the optical transport system which puts some constraints in their deployment. The goal is to have more flexible, controllable, survivable, and comprehensive traffic engineering solutions, as well as an efficient internetworking of IP with Optical layer. The results will accomplish different capabilities, such as the real time provisioning of light paths; the enhancement of network survivability, interoperability, and functionality between vendor-specific optical sub-networks; and the enabling of protection and restoration capabilities in an operational sense.

Different standardization entities have been involved in determining an architectural framework for the interpretabilities of Optical Transport Networks (OTNs), IP networks, SONETs, and ATM backbones.

1.1.1. Layering Architecture Possibilities

The layered design of Optical Transport Networks uses different integrated technologies that interoperate through a client-server relationship for required end-to-end services, which may have different requirements in terms of availability. In contrast, each of these network layers has its own mechanisms for protection and/or restoration to support network survivability. The multi-layer stacks are the result of progressions in cascading technology in IP over OTN, while there are also some new, innovative solutions to provide IP directly over OTN. Fig. 1.1 shows some of the possible technologies for IP over OTN illustrating their layered design.

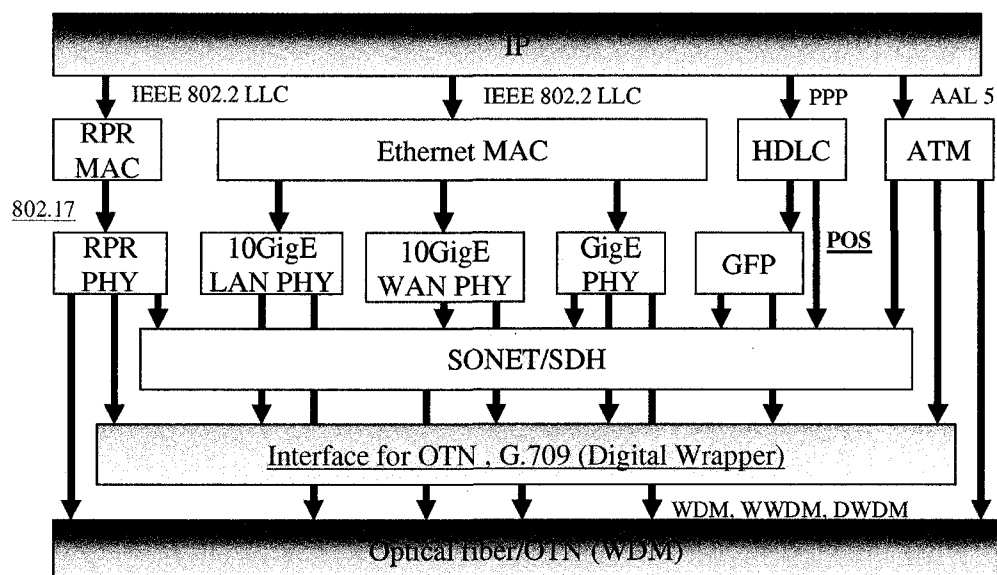


Fig. 1.1: IP to OTN Choices [BON01]

One of the main targets in interfacing IP with an optical network is to make the optical channel driven by IP data paths and traffic engineering techniques. This could not be accomplished without having the very close coexistence of routing and resources management protocols at the two layers [ANSI01]. The long processing time is still to be expected in the multi-layer protocol schemes, however, due to the

large amount of topological and resource information. Multi Protocol Label Switching (MPLS) for IP packets would be the best solution for interfacing the IP world with OTN. Multi Protocol Lambda Switching (MP λ S), where wavelengths are used instead of labels, is formed due to MPLS strength in traffic engineering and OTN control functions. The well developed IP protocols with their integrated control and routing protocols promotes the application of the characteristics of IP intelligence in order to establish reliable end-to-end service over the optical network. It also helps to accomplish the desired management of all network platforms to support the connection between OTNs and the IP for any network or service type.

1.1.2. Network Survivability Schemes

Two main schemes are used to achieve the required survivability of the transport network: network protection and network restoration. These two schemes are used in single-layer as well as multi-layer survivability.

1.1.2.1. Protection

Protection uses a pre-assigned capacity between nodes in order to replace failed or degraded transport entities, and it can be used in both ring and mesh networks.

1.1.2.2. Restoration

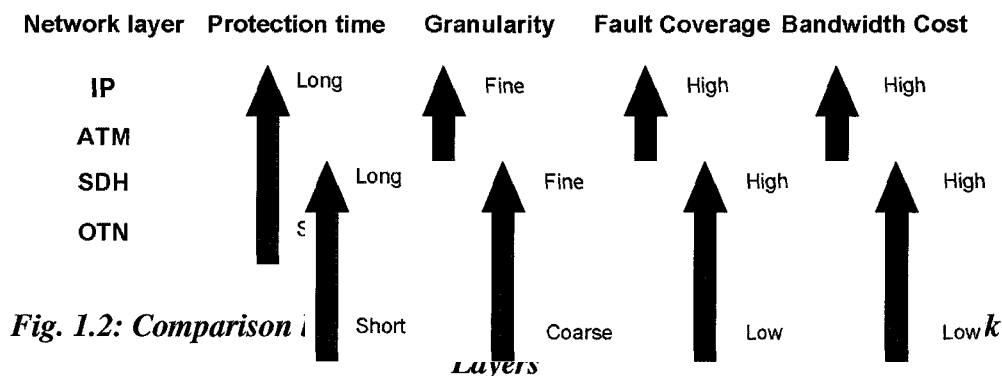
Restoration can use any capacity available between nodes in order to find a transport entity that can replace a failed one. It is based on re-routing algorithms to find a new path to recover failed network entities when a failure occurs.

1.1.3. Multi-layer Survivability Ideology

The main goal of implementing one of the survivability schemes over the others is to minimize the overall costs, either in deploying such a strategy or in reducing downtime penalty expenses.

Every network has its own design in order to fulfill its traffic services, which may require a specific survivability scheme. On the other hand, each survivability scheme has its own characteristics and performance. Moreover, performance changes from one network to another, and one that gives optimum performance on one network will not necessarily do the same on another.

The survivability schemes for the different network layers have significant differences between them in terms of protection time, granularity, fault coverage, and bandwidth cost. A comparison between survivability schemes for different network layers is illustrated in Fig. 1.2 [KAW98C].



From this comparison, the following observations are noted:

- The survivability schemes in the upper layers, e.g. IP restoration, provide good fault coverage for some services, but they may be too slow for others.

- The survivability schemes in the lower layers, e.g. Optical Multiplex Section (OMS) Protection in OTN, are very fast at handling physical layer faults, but the fault coverage may be insufficient for the upper layers' faults.
- The bandwidth cost generally increases from the lower layers to the upper ones due to the increase in signaling and of the complexity of the protocols used.

1.2. Motivation

Today, the challenges in communication networks are not only to provide services to the end-users but also to maintain an acceptable level of service. The main goal of network survivability is to restore the traffic affected by a failure at a network level to the situation before that failure. The complexity of the multi-layer network scheme is that a single failure at a network level may generate a multiple failures in the other different network layers. Thus, before starting the analysis of multi-layer network survivability techniques and providing an analysis of the interactions between them, it is recommended to do an investigation of failures at the network layer and their impact on the service layers (Appendix "A" introduces a survey done on different network failure types and their impacts on the service layers).

Survivability strategies for a single network layer have been investigated for many years in research on communication networks. Some of these networks already have available standards on protection methods and techniques (e.g. SONET). However, it is not always the optimal solution, if we want to achieve a certain level of Quality of Service (QoS) for all traffic types, to use only one survivability technique running in a single network layer without increasing the cost.

Another difficulty with network survivability arises because the optical layer by itself has a restoration/protection capability that requires cautious—coordination with the functions of the higher layer. Because of the high level of multiplexing, one can also expect more problems. Having a large number of higher layers with high traffic rates can cause a large number of alarm messages to flood the network in the case of a failure. Thus, a closer interface between IP and OTN is recommended in terms of packet transfer, routing, and signaling combinations to achieve better network survivability.

1.3. Objective

In multi-layer stacks, the absence of layer coordination between the survivability techniques that exist in each layer can cause unstable operating situations and/or undetermined network operating states. An example to this when there is a major network changes such as a link or node failure (optical physical failure); the amount of IP Link State Advertisement LSA update traffic may be quite significant. The simultaneous or near-simultaneous broadcasting of a large number of LSA messages is commonly referred to as an LSA storm, which in severe cases tends to drive the processor (CPU) utilization to 100% for a longer time period than what is generally accepted. During this period, other important processes within the node may be stalled and even timed-out. For example, the so-called hello packets received at the node would experience a delay, and if this delay exceeds a predetermined threshold the associated link will be declared as down. There may also be other effects of long CPU-busy periods. In a node architecture with an active processor and a standby processor, a switch between the processors may be triggered during an extended

CPU-busy period, which may result in that all the adjacencies, i.e. associations to other adjacent routers, are lost and therefore have to be re-established. Both of these events will lead to more database synchronization and LSA flooding, which in turn may cause extended CPU-busy periods in other routers. This may render the entire network unstable for an extended period of time, or potentially lead to a system meltdown in extreme cases [LIN04].

The objective of this thesis is to precisely define the following using the proposed multi-layer survivability strategies:

1. The survivability functionalities that need to be allocated at each layer; and
2. The coordination between the network layers.

Some of the proposed multi-layer survivability strategies that can be used are:

1. Appropriate selection of survivability schemes;
2. Use of a hold-off time concept;
3. Layer escalation;
4. Sub-network escalation;
5. Scheme escalation;
6. Inter-layer signaling; and
7. Management integration.

1.4. Contributions

This thesis investigates survivability schemes for optical networks that rely only on a single layer, as well as for those that have more than one layer survivability functions and uses different approaches to solve QoS survivability related problems. We have simulated the restoration process of single transport layer: IP, ATM,

SONET and OTN which have been analyzed by similar studies. Also, we have simulated the process of the multi-layer restoration schemes for previously analyzed IP/SONET , IP/OTN and IP-MPLS/OTN by using the hold-off timer concept. We have extended their restoration concept and applied it for IP/OTN and ATM/SONET restoration schemes. Further more, we have introduced IP Restoration/OTN Protection combined multi-layer survivability, IP Restoration/SONET Protection combined multi-layer survivability and IP-MPLS Protection and Restoration/OTN Protection combined multi-layer survivability. In this thesis, we have combined the analyses with simulations to form a comprehensive study for the IP over OTN survivability across different architectures. The study focuses on four of the most commonly used network architectures of the IP over OTN architecture possibilities:

1. IP/ATM/SONET/OTN reference architecture (this is chosen to be a reference to the other architectures);
2. IP/POS/OTN architecture;
3. IP/GbE/OTN architecture; and
4. IP-MPLS/OTN architecture.

The comprehensive analysis of the different architectures has illustrated that the integration of the protection functions in the OTN or SONET layer (e.g. OCh protection) with the IP restoration functions is a superior strategy for multi-layer survivability

1.5. Thesis Organization

Chapter 1 provides an introduction and background. Appendix A summarizes an analysis of network failures and describes the survivability measures taken. Chapter 2

presents the available survivability of different network transport layers. The analysis done for those layers are demonstrated in Appendix B. Chapter 3 describes multi-layer survivability solutions and illustrates the four network architectures chosen with their available survivability functions. The different encapsulation methods used to form these architectures are described in Appendix C. Chapter 4 demonstrates the performance evaluation done through network simulations. Chapter 5 concludes with remarks on this study and recommends further research work.

Chapter 2: Survivability in Network Transport Layers

This chapter will introduce the available survivability schemes for optical networks that rely only on a single layer, as well as for those that have more than one layer but use only one-layer survivability functions.

2.1. Survivability in the Optical Layer

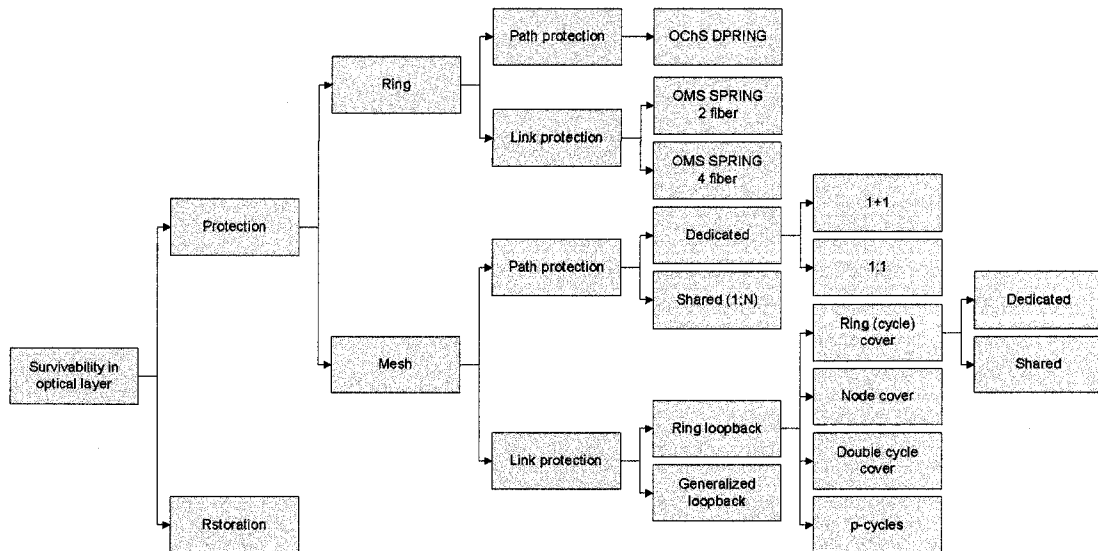


Fig. 2.1: Optical Layer Survivability Techniques [MAL02]

Fig. 2.1 illustrates the different survivability techniques that can be implemented in optical networks with different topologies [FUM00].

2.1.1. Protection in the Optical Layer

According to ITU-T G709 specifications, automatic protection can be performed only at the OMS and OCh sub-layers, which will be described in detail hereafter.

2.1.1.1. OMS Protection

OMS Protection can be viewed as a bulk protection in which the protection is done for all wavelengths carried by the fiber, i.e. the protection is done at the fiber level. The advantages of using this kind of protection are that it is fast, simple, and robust. On the other hand, the disadvantages of using this kind of protection are its coarse granularity, and the low efficiency of utilization. Fig. 2.2 shows one of the possible configurations of the OMSP. This configuration can provide protection for the possible failures of fiber cables and optical amplifiers. On the other hand, it cannot provide protection for the possible failures of transponders, OTN MUX and DEMUX, and IP router interface cards.

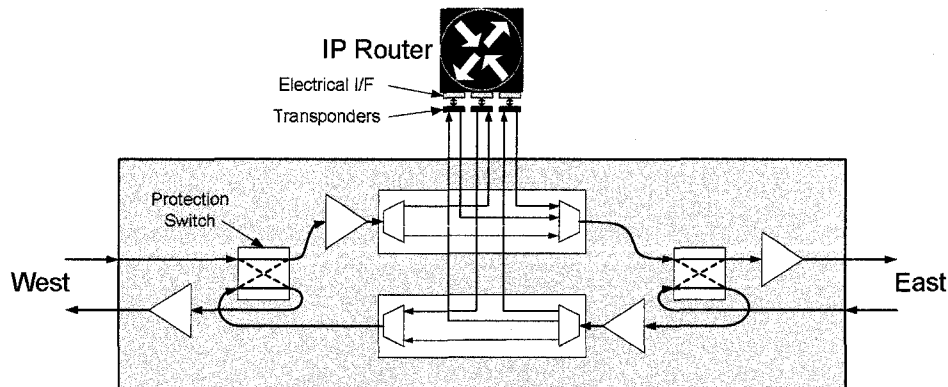


Fig. 2.2: Possible Node for OMSP in a Ring Configuration

2.1.1.2. OCh Protection

OCh Protection differs from OMS Protection. OCh protection does not cover all the wavelengths carried by the fiber but only those selected. In case of failure, the protection is done automatically by switching these selected wavelengths (channels) to the pre-assigned wavelengths. The advantages of using this kind of protection are efficient usage of the network capacity i.e. high efficiency of network utilization, and fine granularity. On the other hand, the disadvantages of using this kind of protection are that it is complicated, and provides low network utilization efficiency.

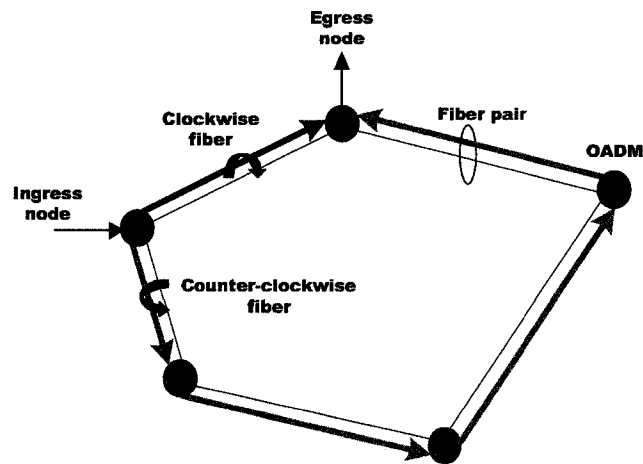


Fig. 2.3: 1+1 OChP Ring

Fig. 2.3 and Fig. 2.4 show one of the possible configurations of the 1+1 OChP, a Sub Network Connection Protection (SNCP). This is the main protection method used in current OTN networks. This configuration can provide protection for the following possible failures: OTN MUX and DEMUX, optical amplifiers, and IP router interface cards. On the other hand, it cannot provide protection for the possible failures of transponders and IP routers.

The second possible configuration of the OChP (as shown in Fig. 2.5) is Trail Protection. This configuration can provide protection for the following possible failures: transponders, OTN MUX and DEMUX, optical amplifiers, and IP router interface cards. On the other hand, it cannot provide protection for the possible failure of IP routers.

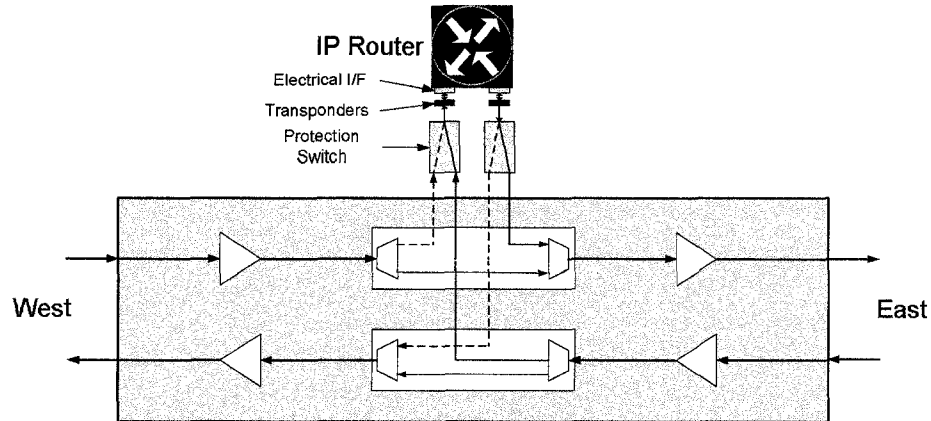


Fig. 2.4: SNCP (OChP) Node in a Ring Configuration

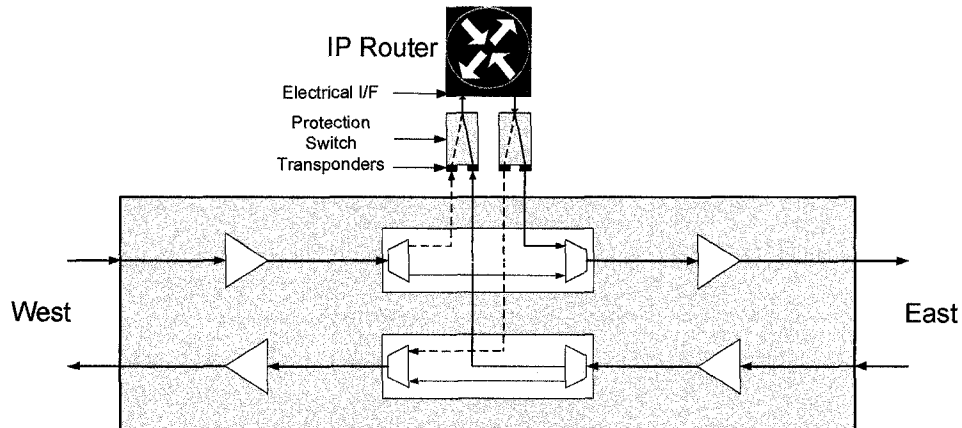


Fig. 2.5: Trail Protection (OChP) Node in a Ring Configuration

There is a difference between these two types of protection. In the OCh trail, the protection is done by duplicating the transponder cards (as shown in Fig. 2.6b). On the other hand, in the SNCP, the optical switches are placed between the transponder and the OTN filters, and this splits/combines the wavelengths (Fig. 2.6a).

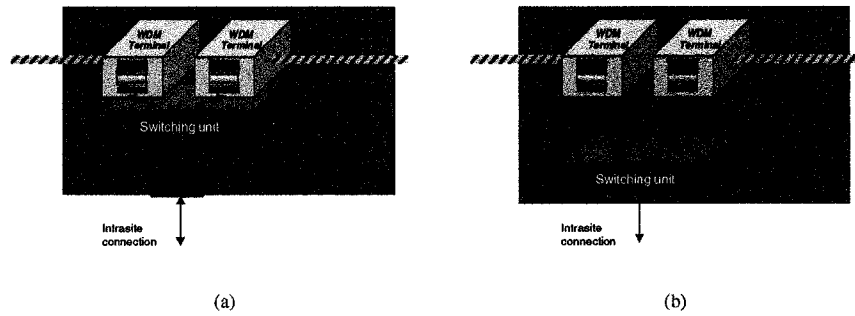


Fig. 2.6: Architecture of OADM for 1+1 OCh Protection: (a) SNCP and (b) Trail Protection

Trail Protection apparently provides better performance from the survivability point of view; however, it increases the cost because it requires more equipment to be used in this configuration.

2.1.1.3. Dedicated and Shared Protection

The protection in the optical sub-layer is either OMSP or OChP, which in turn can be either dedicated (DP) or shared (SP).

2.1.1.3.1 Dedicated Protection

DP is in the form of 1+1 (as shown in Fig. 2.7) where the working traffic is copied to another route. At the receiver side, the route that provides lower error rate is selected. This means that the other route is in use by this protection method 100% of the time. In other words, the network protection capacity is equal to the network transmission capacity, and each of them is half of the network total capacity [ZHO00]. The advantages of using this kind of protection are that it is fast, simple, and has high QoP utilization. On the other hand, the disadvantage of using this kind of protection is its poor utilization of the network capacity.

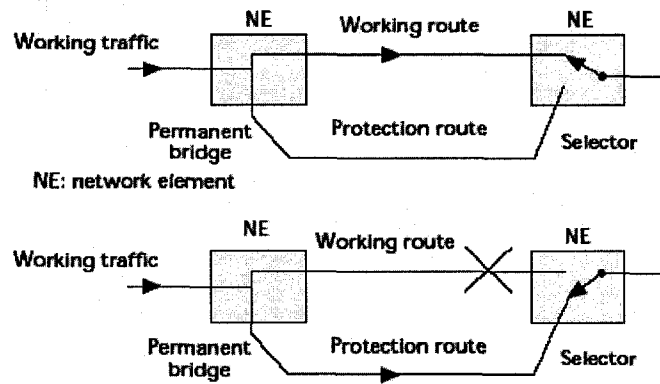


Fig. 2.7: Architecture of 1+1 Protection Schemes [ZHO00]

2.1.1.3.2 Shared Protection

Shared protection can be in the form of 1:1 (as shown in Fig. 2.8), 1:N, or k:N. One or more traffic routes are used to protect the working traffic(s). The shared protection routes may be used to carry extra less important traffic(s) [ZHO00].

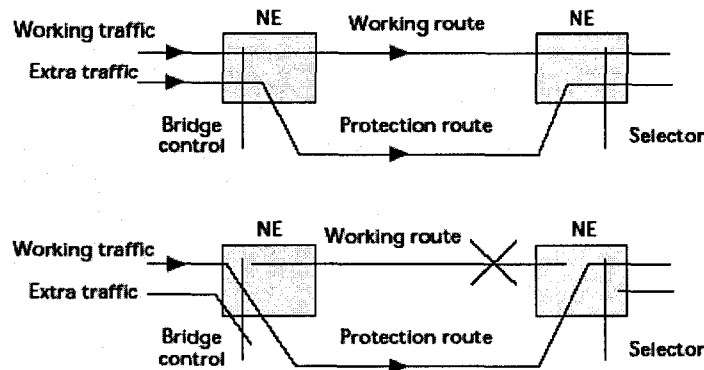


Fig. 2.8: Architecture of 1:1 Protection Schemes [ZHO00]

The advantage of using this kind of protection is its efficient utilization of network capacity. On the other hand, the disadvantage of using this kind of protection is its complications.

Both dedicated and shared OChP methods are implemented in OTN in both peer-to-peer and OADM ring networks. However, only the dedicated OMSP method is implemented in the current peer-to-peer networks. The existing OADMs usually

implement only 1+1 OCh protection, which means that these networks either support this type of protection or do not provide any protection at all.

2.1.1.4. Link and Path Protection

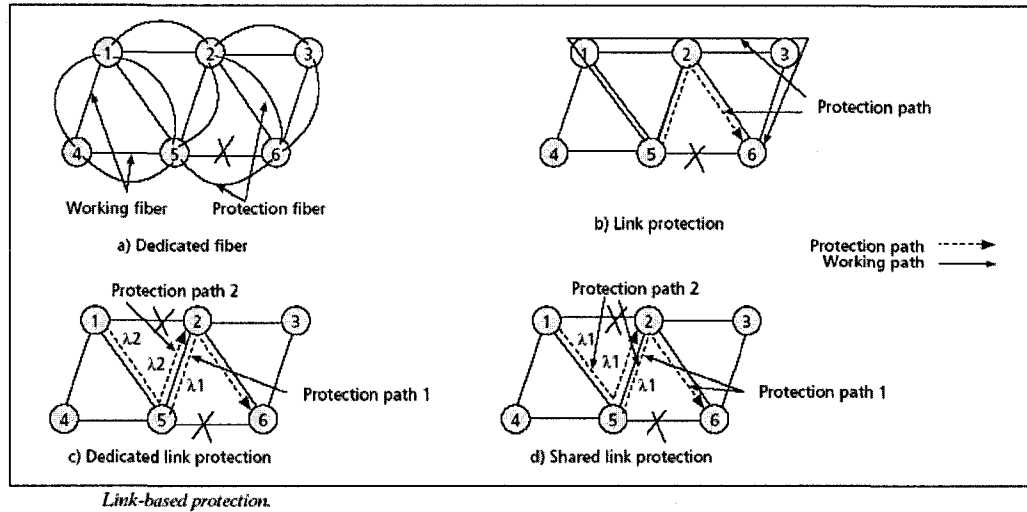


Fig. 2.9: Link-based Protection [ZHO00]

In OTN, protection can be done either on the link (the connection between any adjacent nodes that may be OADMs) as shown in Fig. 2.9, or on the path (the complete route from the source node to the destination node) as shown in Fig. 2.10. Basically, the different protection schemes described before, OCh and OMS, either dedicated or shared, are mainly link-based type of protection. The protected link (or path) must be disjointed with the working link (or path). Also, for any two working paths having one or more links sharing the same risk of failure, their protected paths must be disjointed (this is known as SRLG constraints).

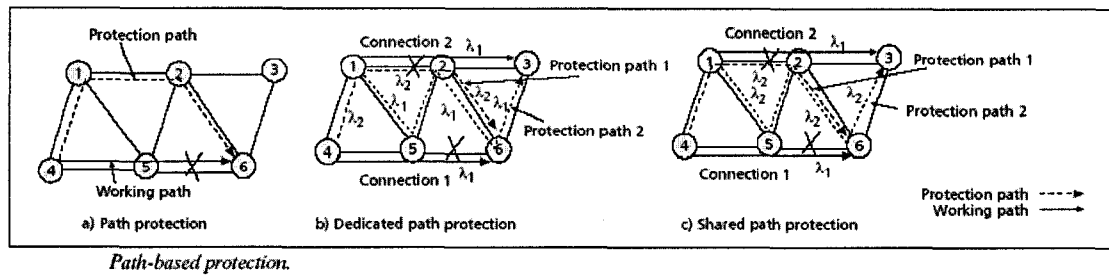


Fig. 2.10: Path-based Protection [ZHO00]

2.1.2. Restoration in the Optical Layer

Restoration can use any capacity available between nodes in order to find a transport entity that can replace the failed one. Restoration is based on re-routing algorithms to find a new path to recover failed network entities at the time the failure occurs. The algorithms are those acting in levels higher than the network layer where the actions are applied. In general, the restoration process follows the following steps:

1. Detection of the failure,
2. Dissemination of the alarms
and control messages,
3. Re-Routing,
4. Network updates,
5. Return to normal.

2.1.2.1. Centralized and Distributed Restoration Control Architectures

Restoration architecture can be classified according to the locations of its action control, as either centralized or distributed. The restoration process control in the centralized architecture is operated from one unit that may be integrated with network management. On the other hand, the control of the restoration process in distributed architecture is operated from many units spread throughout the network and may be integrated within some network elements. The advantages of distributed restoration over centralized restoration are that it is faster and more flexible while the advantages

of centralized restoration over distributed restoration are that it has better network management and a lower complexity of network elements.

2.1.2.2. Dynamic and Pre-planned Restoration Control Architectures

In dynamic restoration, re-routing activities are done after receiving a restoration request based on the network status at that time. In pre-planned restoration, however, the re-routing activities are done after receiving a restoration request according to a pre-determined route determined by the network restoration management. The advantages of pre-planned restoration over dynamic restoration are that it is faster and has better network management, while the advantages of dynamic restoration over pre-planned restoration are that it does not require continuous network management activities to update re-routing tables, and demonstrates better use of network resources [ALB06].

2.1.2.3. Adjacent-node, Intermediate Node and End-to-end Restoration Types

In end-to-end restoration, re-routing is done by finding a completely new path between end nodes of the affected traffic. In adjacent-node restoration, re-routing is done by finding another link between the nodes for the affected link traffic. In intermediate-node restoration, re-routing is done by finding another link/path between any intermediate nodes to re-route the affected traffic between the two end nodes.

A comparison between adjacent node, intermediate node, and end-to-end restoration types is listed in Table 2.1.

Table 2.1: Comparison of Adjacent Node, Intermediate Node, and End-to-End Restoration Types

Restoration Type	End-to-End	Adjacent-Node	Intermediate-Node
Network resources required	Few	More	Moderate
Resource sharing provided	High	Low	Moderate
Restoration speed	Slower	Faster	Moderate
Capacity reserved	~60%	~80%	~70%

In today's optical networks where each node considered, including an Optical Cross-Connect (OXC), restoration techniques can be implemented at the OCh layer. It can also be implemented using O-E-O cross-connects designed to deploy fast restoration. The use of OCh restoration allows us to define a priority classes.

2.2. Survivability in the IP Layer

The survivability of the data transferred through the Internet is the result of the coordination between the routers and hosts. This kind of coordination is accomplished through routing protocols that are responsible for collecting, disseminating, and processing routing-related information.

2.2.1. IP Protection

IP protection can be achieved by duplicating the core routers. Each group of either the working or backup routers is connected by dedicated fiber (OMSP) or separate optical channel (OChP), as shown in Fig. 2.11. The access routers are connected to both the working and the backup routers. In this scenario, in case of a failure in one of

the working routers, service restoration is done at the IP level by switching to the backup router.

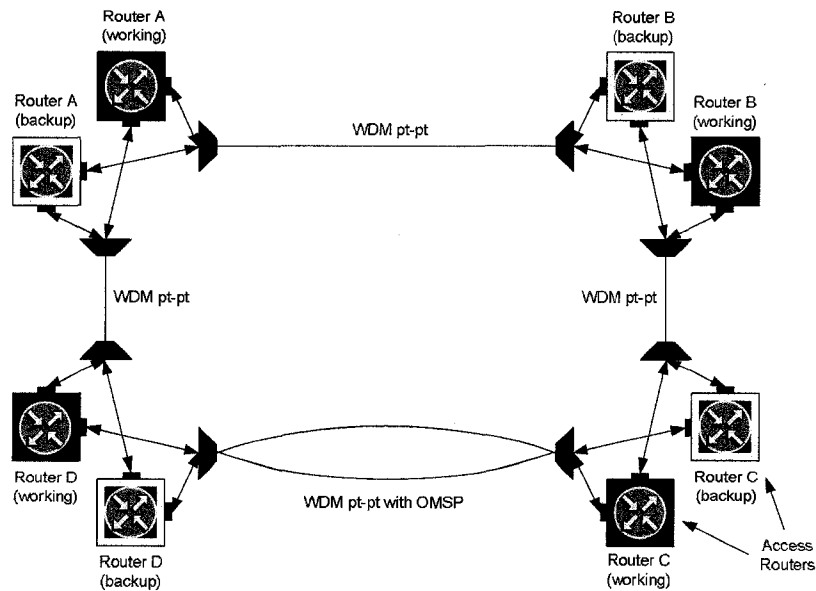


Fig. 2.11: Protection against Router Failures by Duplication

There are other scenarios in which both routers A and B are sharing the load, and in the case that one of them fails, the other will take over its load.

2.2.2. IP Restoration

IP restoration is achieved by the routing protocols' capabilities against single or multiple failures. The main advantages of the survivability achieved by IP restoration are that it is flexible and robust, and has fine granularity. On the other hand, it suffers from one important disadvantage: its slow processing capability.

In general, the reconstruction time depends on many factors such as the complexity of the network (i.e. the number of nodes and interconnections) and the type of protocols used. Although the restoration time, which typically ranges from seconds to

minutes, is considered relatively long, the detection time is a multiple of that and thus makes the total time of survivability considerably longer.

2.3. Survivability in SONETs

SONET survivability has three known network schemes:

- 1) Protection switching: In this scheme, the end-to-end terminal equipment established a pre-assigned substitute connection without the assistance of network management control functions;
- 2) Self-healing: In this scheme, any terminal equipment may establish a pre-assigned substitute connection without the assistance of network management control functions;
- 3) Rerouting: In this scheme, the terminal equipment establishes a pre-assigned substitute connection with the assistance of the network management control functions.

2.3.1. SONET Protection with APS

The SONET line connections use APS in one of the following two architectures:

- 1) 1: N ($1 < N < 14$): Also called shared protection, the N working lines are to be bridged to a single protection line. Fig. 2.12 shows an example of 1:N SONET APS. In contrast to asynchronous APS optical systems that use out-band signaling, the SONET APS protocol uses in-band signaling K1 and K2 bytes within the SONET line overhead. K1 byte carries requests for switching action, while K2 byte transfers confirmation that the connection has been bridged onto the protection line.

In this architecture, both the head and the tail ends have to simultaneously bridge to the protection line.

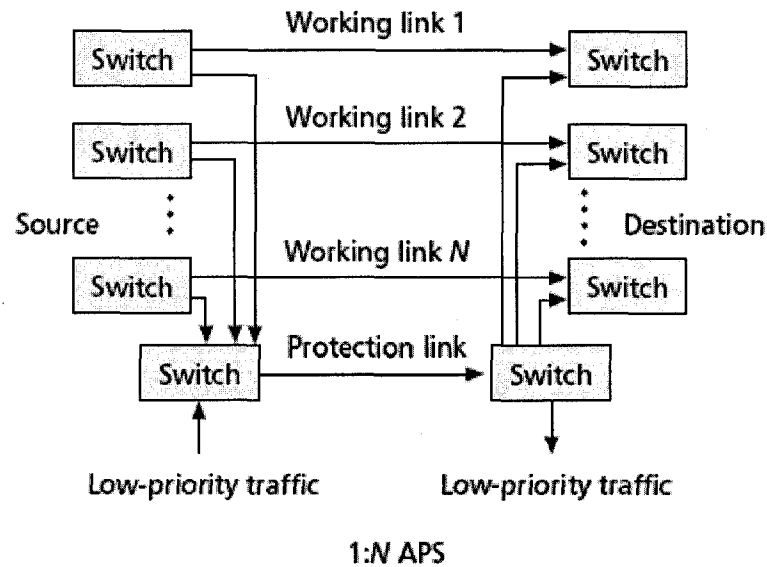


Fig. 2.12: SONET 1:N APS [ZHO00]

- 2) 1+1 Diverse Protection (as shown in Fig. 2.13): Also called dedicated protection, it differs from 1:1 APS/DP switching in that the head ends are permanently bridged. In this architecture, only the tail end can receive the switching decision. The K1 byte in the bidirectional switching is used to convey the signal state to the head end. After the action is done by the tail end, it sends the K2 byte to the head end.

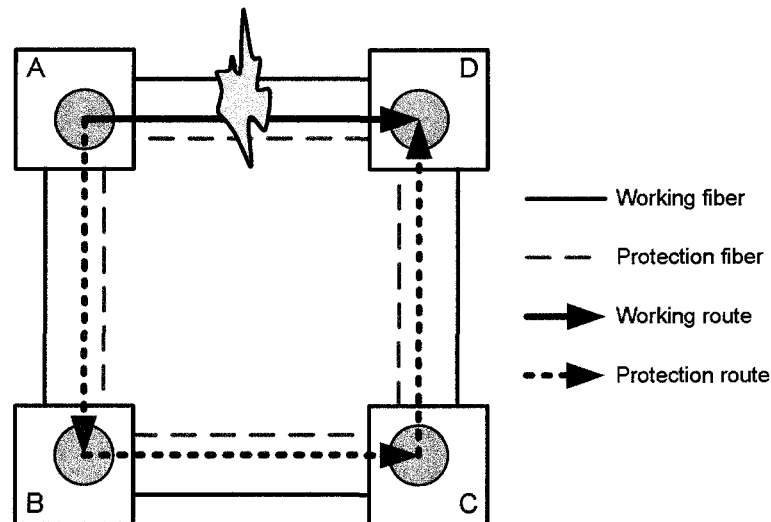


Fig. 2.13: SONET APS/DP (Dedicated Protection) 1+1 Protection of the Path AD [MAL02]

2.3.2. SONET Protection in the Self-Healing Rings

The SONET rings are categorized according to their routing architecture as follows (also they are illustrated in Fig. 2.14):

1. Unidirectional, where the protection route is in the direction opposite to the working traffic. Only one fiber is required for this protection route.
2. Bidirectional, where the working traffic is in two opposite physical ring routes carried by two fibers. There are two types of this kind according to the ring topology deployed:
 - a. BSHR/2: If there are no extra fibers for protection, the protection can be done as USHR;
 - b. BSHR/4: The protection routes use another two fibers that are similar to the working loops.

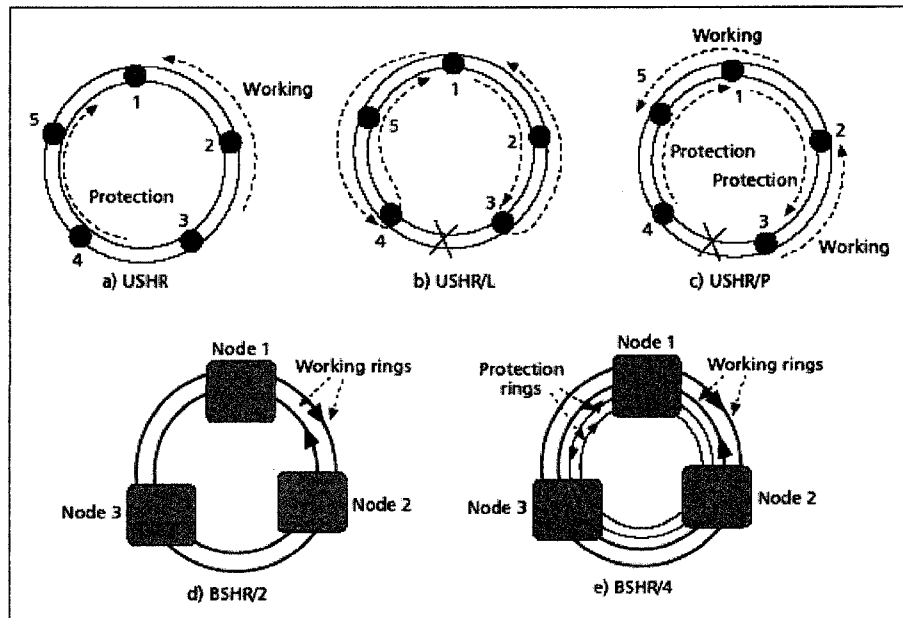


Fig. 2.14: SONET SHR [ZHO00]

USHR is used in access and peripheral networks where the traffic is centered in one location due to its economical design. BSHR is used in areas in which there is uniform traffic as well as in inter-office networks with a non-hubbing structure. Fig. 2.15 shows LTE with BSHR/4 in normal working condition, while Fig. 2.16 and Fig. 2.17 show the LTE with a working link in failure and with both working and protection links in failure respectively.

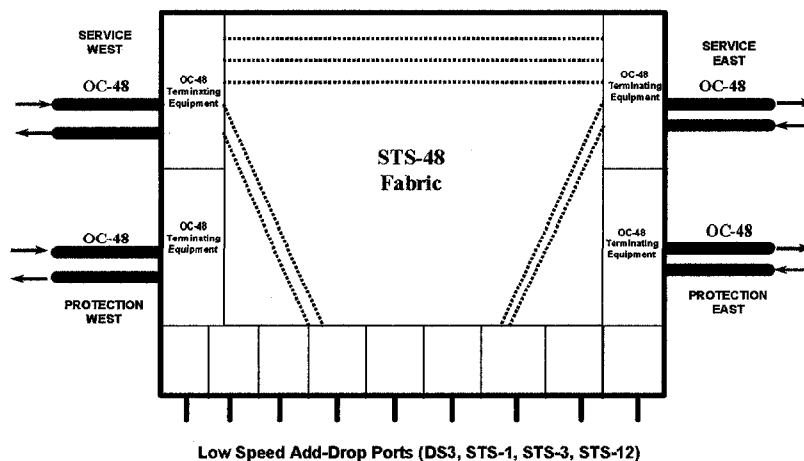


Fig. 2.15: LTE with BSHR/4 in Normal Working Condition

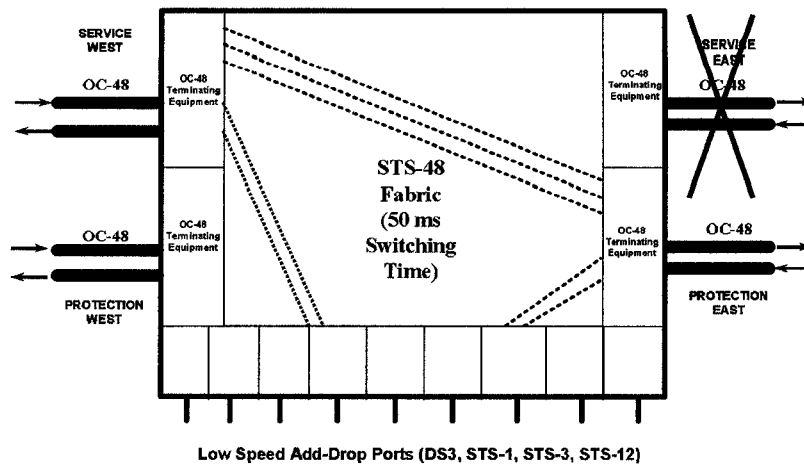


Fig. 2.16: LTE with BSHR/4 with a Working Link in Failure

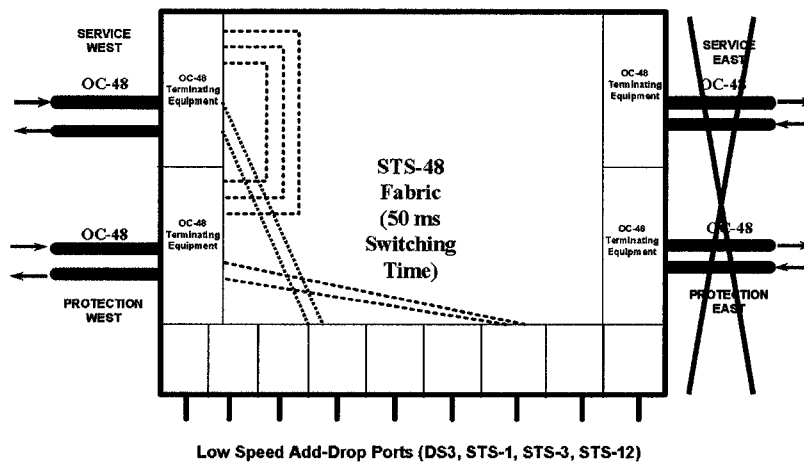


Fig. 2.17: LTE with BSHR/4 with Both Working and Protection Links in Failure

A comparison between SHR schemes is listed in Table 2.2.

Table 2.2: Comparison between SHR Schemes

SHR Architectures	ADM Type	Carry Demand	Node Component Costs	System Complexity
BSHR/4	Basic ADM	More	Higher	Simple
BSHR/2	ADM/TSI	Medium	Medium	Complex
USHR	Basic ADM	Lower	Lower	More complex

2.3.3. SONET Restoration in DCS Self-Healing Mesh Networks

Digital Cross-Connect Systems (DCS) mesh network has the following two configurations. The first is centralized control, in which the network reconfiguration process is managed by the center controller and executed by several Local Exchange Carriers LECs and Long Distance Carriers LDCs. The second is distributed control, in which the network reconfiguration process is managed and executed at each DCS node.

The restoration process may be done at either the line level or path level. The DCS self-healing network is economically attractive in areas where high demand and high connectivity are involved.

2.3.4. Relative Comparisons among the SONET APS/DP, SHR, and Self-healing Networks (SHN)

The APS/DP and rings have the ability to restore services rapidly. The two choice criterions between the two systems are network size and cost. APS/DP systems are more appropriate in situations where point to point is highly demanded. On the other hand, ring are appropriate in situations where the expansion rate is stable and reasonably slow.

The DCS Self-healing Network SHN needs less protection capacity but takes longer restoration time and requires more complex planning and operational systems. The spare capacity for the DCS SHN is mainly due to sharing of spare capacities across the entire network. This system provides great advantages when it functions appropriately but may cause many problems in much wider area when a software

failure occurs. To avoid taking the entire network down due to software failures, partitioning may be needed to be done in order to improve the DCS networks reliability. A comparison between the SONET APS/DP, SHR, and DCS self-healing networks is listed in Table 2.3.

Table 2.3: Relative Comparisons between the SONET APS/DP, SHR, and DCS Self-healing Networks.

Attributes	APS/DP	SHR/ADM ring	SHN
Network size	2 nodes	Up to a few tens of nodes	Global
Spare capacity needed	Most	Moderate	Least
Per node cost	Moderate	Lowest	Highest
Fiber counts	Highest	Moderate	Moderate
Connectivity Needed	Lowest	Moderate	Most
Restoration time	~50 ms	~50 ms	~2 Seconds
Software complexity	Least	Moderate	Most
Protection against major failure	Worst	Medium	Best
Planning/operations complexity	Least	Moderate	Most

2.4. Survivability in ATM

In ATM, the Virtual Path (VP) has some unique characteristics. The most striking characteristic is the independence of its route and bandwidth establishment, which allows a VP route to be established without assigning its bandwidth along the path. This is not the case in SONET networks, in which a digital path is established by assigning a time slot of the STS frame to each cross-connect on the path and thus allows, only fixed bandwidth digital paths to be established. Because of this

hierarchy, if a network failure happens, the VP manager starts to perform the restoration. If for any reason the VP manager can not perform this task, the Facility Network (FN) has to initiate a facility network planning process.

2.4.5. ATM Protection

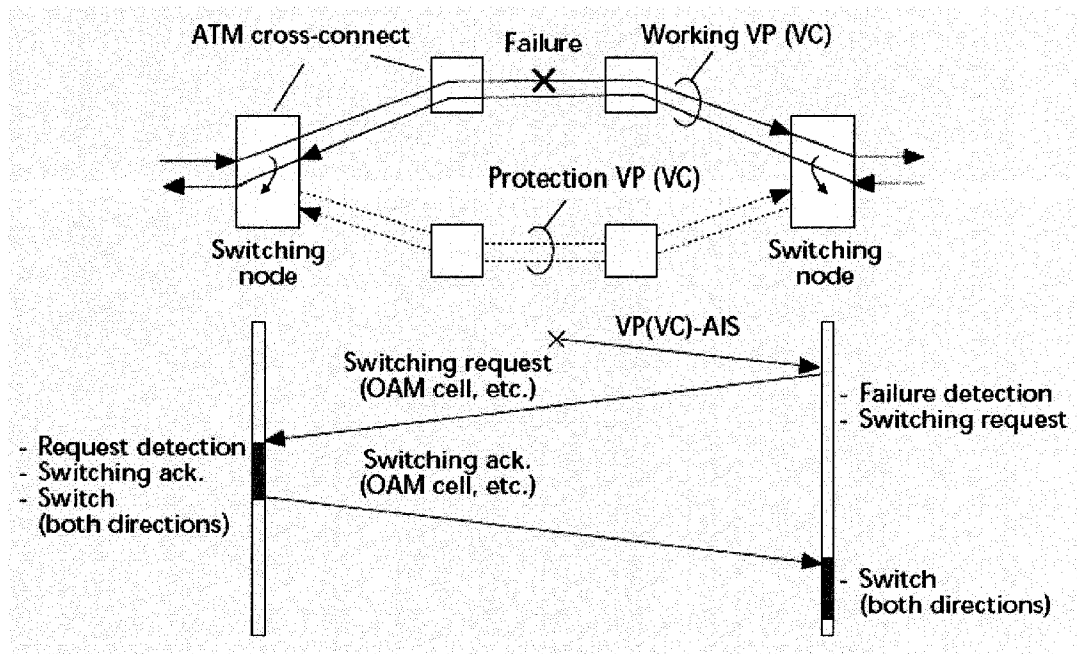


Fig. 2.18: ATM 1:1 APS Protection [KAW98C]

The APS mechanism can be applied to ATM networks using VPs or VCs as links (protection units). APS schemes are classified into three types [KAW98C]:

- 1) 1 + 1 APS: VP-APS restoration is almost the same as the SDH section APS (~ 50 msec) [AND94A].
- 2) 1 : 1 APS (as shown in Fig. 2.18): VP-APS has been discussed in ITU-T SG13 (WP3 Question 6/13) as a basic restoration function in ATM networks [ITU97A]. 1:1 APS is more effective than 1 + 1 APS in ATM networks. This is because low priority traffic, e.g., unspecified bit rate (UBR) and adaptive control traffic such as Available Bit Rate (ABR), can use the backup path.

- 3) M : N APS: The N working paths are bridged to the M protection paths.

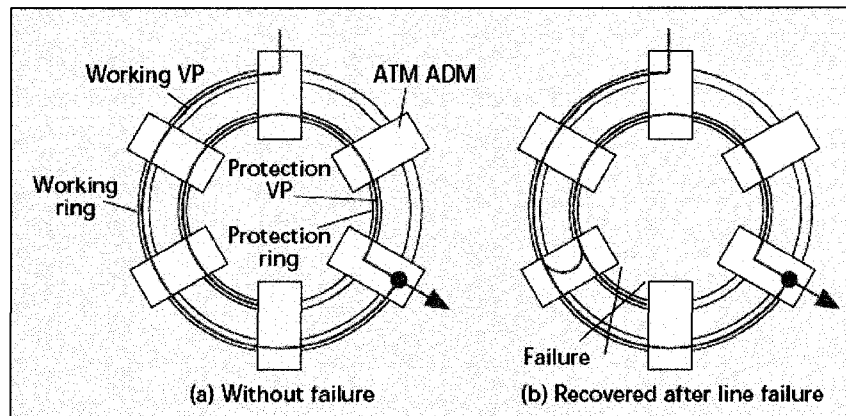


Fig. 2.19: ATM Self-healing Ring (SHR) [KAW98C]

- 4) Self-healing Ring SHR (as shown in Fig. 2.19): It provides rapid restoration for ring topology networks and simplifies the restoration algorithm used. The desired SONET performance (~ 50 ms) can be achieved. The simplicity of the SHR design reflects on the network management used and this decreases the administration cost.
- 5) Self-healing Network SHN (as shown in Fig. 2.20): This scheme uses distributed control restoration functions for DCS-based networks in which there are no topological restrictions. SHN pre-determines the optimal alternate route in the network planning phase, and pre-assigns a backup VP to each VP before any failure occurs.

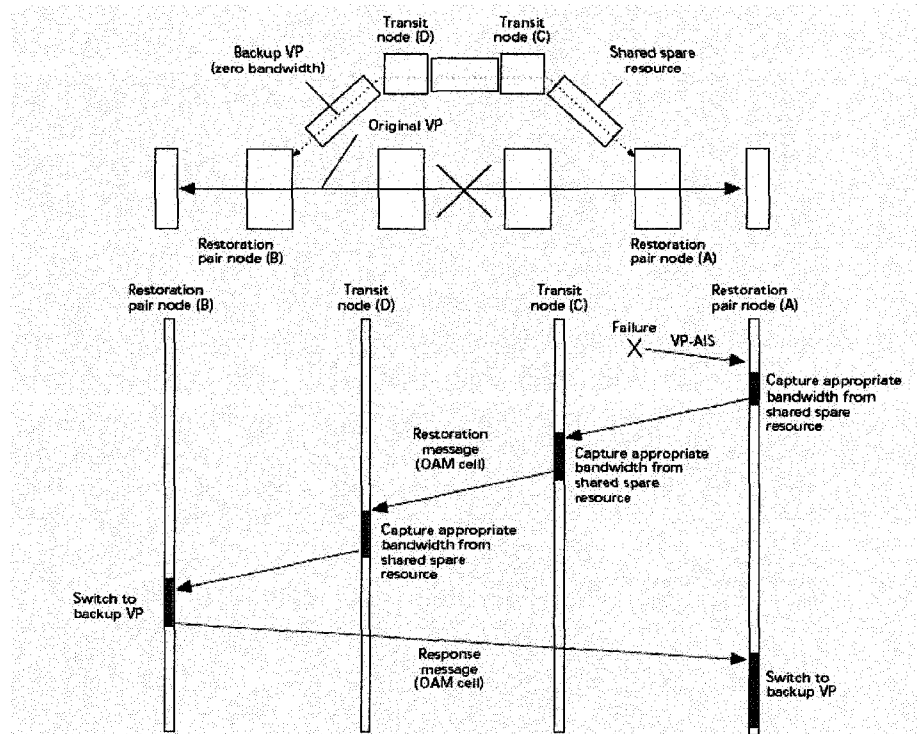


Fig. 2.20: ATM Self-healing Network (SHN) [KAW98C]

6) Failure Resistance Virtual Path FRVP (as shown in Fig. 2.21) [KAW98A]

[KAW98B]: An efficient and reliable scheme is offered that provides failure free transmission in spite of network failures. The idea behind it is to establish parallel transmissions (Redundancy) between the end points. The receiver selects the Error-free cell among the received ones. The assigned VPs satisfy the SRLG constraint to be immune to fiber-cut failures. The transmitter inserts index cells into the data cells to provide the cell order at the receiver.

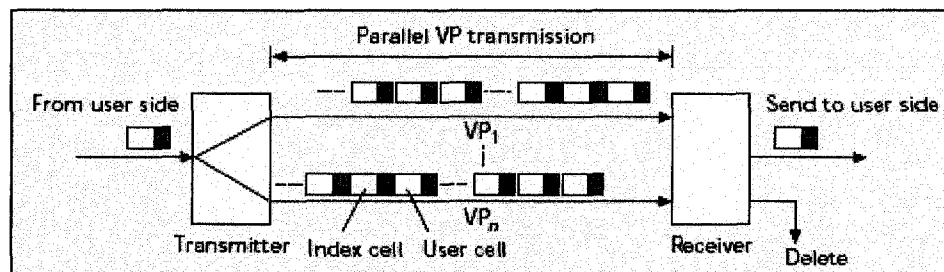


Fig. 2.21: ATM Failure Resistance Virtual Path FRVP [KAW98C]

2.4.6. ATM Restoration

Path restoration in ATM networks is achieved by re-routing cells from the failed VP to a backup VP after a failure's occurrence. The most motivating characteristic is its ability to pre-establish backup paths using zero bandwidth VPs. Path restoration is done by capturing the bandwidth of the backup VP from shared spare resources in each link [VEI97].

After the detection of a failure, nodes start setting up backup routes by flooding AIS messages. Enhancements are done to these methods to reduce the number of messages in order to increase the speed of restoration. A Hop-limit technique can be one of the proposed solutions. With an analogy to the IP, several schemes are proposed in order to select the best route.

2.4.6.1. Two-step Restoration Scheme

The restoration process has two requirements:

- 1) Initialize a fast, optimally configured VP that incurs the smallest amount of service interruption upon a possible, upcoming failure;
- 2) Achieve optimal flow planning.

These two requirements contradict each other since optimal flow calculation introduces a computational delay that does not comply with the first requirement.

In order to accommodate these contradicting requirements, the VP manager uses a two-step restoration scheme (as shown in Fig. 2.22):

- 1) **Fast Restoration:** Upon failure, the VP restoration manager performs a fast restoration process to speed up the failure recovery;

- 2) Network-wide Restoration: After the fast restoration is done, the VP planner unit calculates an optimal VP assignment for the latest network topology and the VPs are changed accordingly (network wide restoration).

Although this solution does not produce the most favorable results demanded, it is still accepted since there are no others that provide better performance. The performance may degrade in the case of multiple failures, but since the probability of more than one failure in a short time is very small, this factor is not taken into consideration. Since the number of paths per link is relatively large and can reach a maximum of 4096 VPs/link, the number of paths that can be affected by a single failure is consequently large. This can be a nightmare for the network management.

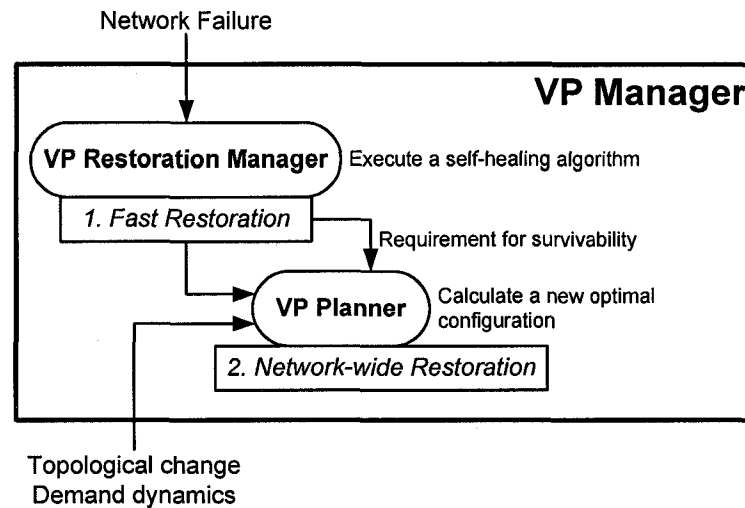


Fig. 2.22: ATM Two-steps Restoration Mechanism

A comparison between ATM protection and restoration is listed in Table 2.4.

Table 2.4: Comparison between ATM Protection and Restoration [KAW98C]

	ATM Restoration	ATM Protection
Restoration rapidity	Slow (route searching)	Fast
Algorithm and message transmission protocol	Complex	Simple
Number of generated messages	Large	Small
Restoration segment	Between link terminator (difficult to restore between path terminator)	Between link terminator (any node along the path)
Required spare resource	Large	Small
Node failure restoration	Difficult	Easy (except failure of restoration pair node)
Support of process identification and interruption	Difficult	Easy
Backup path management	Not required (only at failure occurrence)	Required
Spare resource management	Necessary if high ratio of restoration needed	Proper management of spare resource on the backup route is necessary
Flexibility against multiple or unforeseeable failures	High	Low

2.4.7. Survivability Quality of Service

Survivability Quality of Service (SQoS) is a better measure of survivability in ATM networks. It is used as a resource management control performance indicator.

2.5. Survivability in the MPLS (GMPLS)

MPLS as a relatively new backbone technology must provide satisfactory services for the network traffic including the protection of the traffic carried on the LSPs. MPLS protection switching refers to the ability of the MPLS layer to rapidly and fully restore traffic during any changes to the condition of the MPLS layer [ALB06]. Fast MPLS layer protection should be as good as the 50 ms restoration time of the SONET layer.

2.5.8. MPLS Protection

MPLS Protection (also called MPLS Fast Re-routing) is a local network resiliency mechanism. It is actually a feature of RSVP Traffic Engineering (RSVP-TE).

In MPLS Protection, there is a pre-established protection path for each working path, with resources (bandwidth, buffers) that are reserved (i.e. not in use) or used only by low priority traffic (if there is no failure on the working path). The node that redirects the traffic onto the preset backup path is called the Point of Local Repair (PLR), and the node where the backup LSP merges with the primary LSP is called the Merge Point (MP). This mechanism (local protection) provides faster recovery because the decision about recovery is made strictly locally. For comparison, when recovery mechanisms are employed at the IP layer, restoration may take several seconds and this is unacceptable for real-time applications (such as VoIP). In contrast, MPLS local protection meets the requirements of real-time applications with recovery times comparable to those of SONET rings [YIN01].

The general concepts of protection switching are valid for MPLS protection as well. In particular, the following methods may be used in the protection schemes:

- Protection mode (preventive or non preventive); and
- Protection switching options (1+1, 1: n, m:n).

2.5.9. MPLS Restoration

In MPLS restoration, the backup path is created as soon as a failure is detected. By using this method, the network resources are better employed but at the expense of a longer restoration time. From the point of view of management, the types of restoration (as illustrated in Fig. 2.23) may be classified as follows [ZHA02]:

- 1) Global, End-to-end or Centralized Restoration: Upon the detection of the failure of the primary path, a backup path is created between the source and destination nodes. It can be considered a slow process but it utilizes better the network resources since it requires only a single protecting path for each working path;
- 2) Local or Distributed Restoration: Upon detecting the failure of the primary path, a backup path is created between the two nodes of failure. Here the restoration is established by each LSR along the working path in a distributed way.

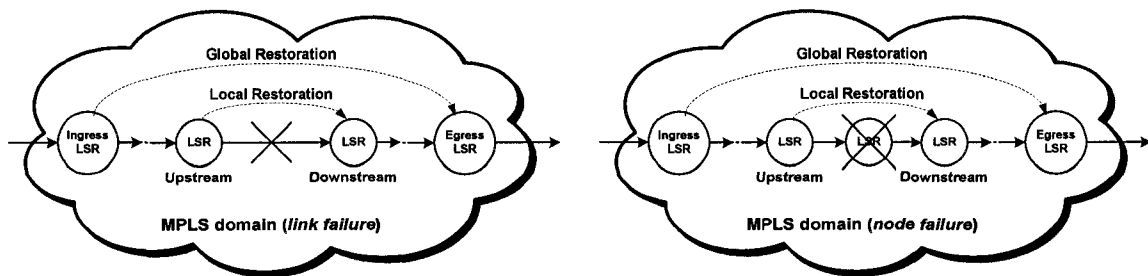


Fig. 2.23: Restoration Schemes in IP-MPLS [ZHA02]

2.5.9.1. Failure Notification

The traffic sending upstream LSRs alongside the affected working LSP must be notified after failure detection. Sending an explicit Failure Indication Signal (FIS) back to them can be one method of notification. Another method is realized when the downstream LSR returns the Keep Alive message sent by the upstream LSR with the optional failure notification field set. The above two methods use “out-of-band” notification. However, it is also possible to use “in band” notification.

2.5.9.2. Restoration Time

According to the network size, topology, and the number of LSPs affected by the failure, the MPLS restoration times may vary considerably. Based on practical results, the restoration time varies between 6.1ms and 185 ms.

2.5.10. MPLS Restoration Practice

The MPLS Restoration re-routing process goes through the following set of events, which is shown in Fig. 2.24.

Critical choices involve the frequency of HELLO messages and the value of T_{fail} . The frequency of the HELLO messages is usually set to 5 ms, the interval for failure detection T_{fail} to 20 ms (4 HELLO messages lost), and the interval for failure recovery T_{repair} set to 500 ms.

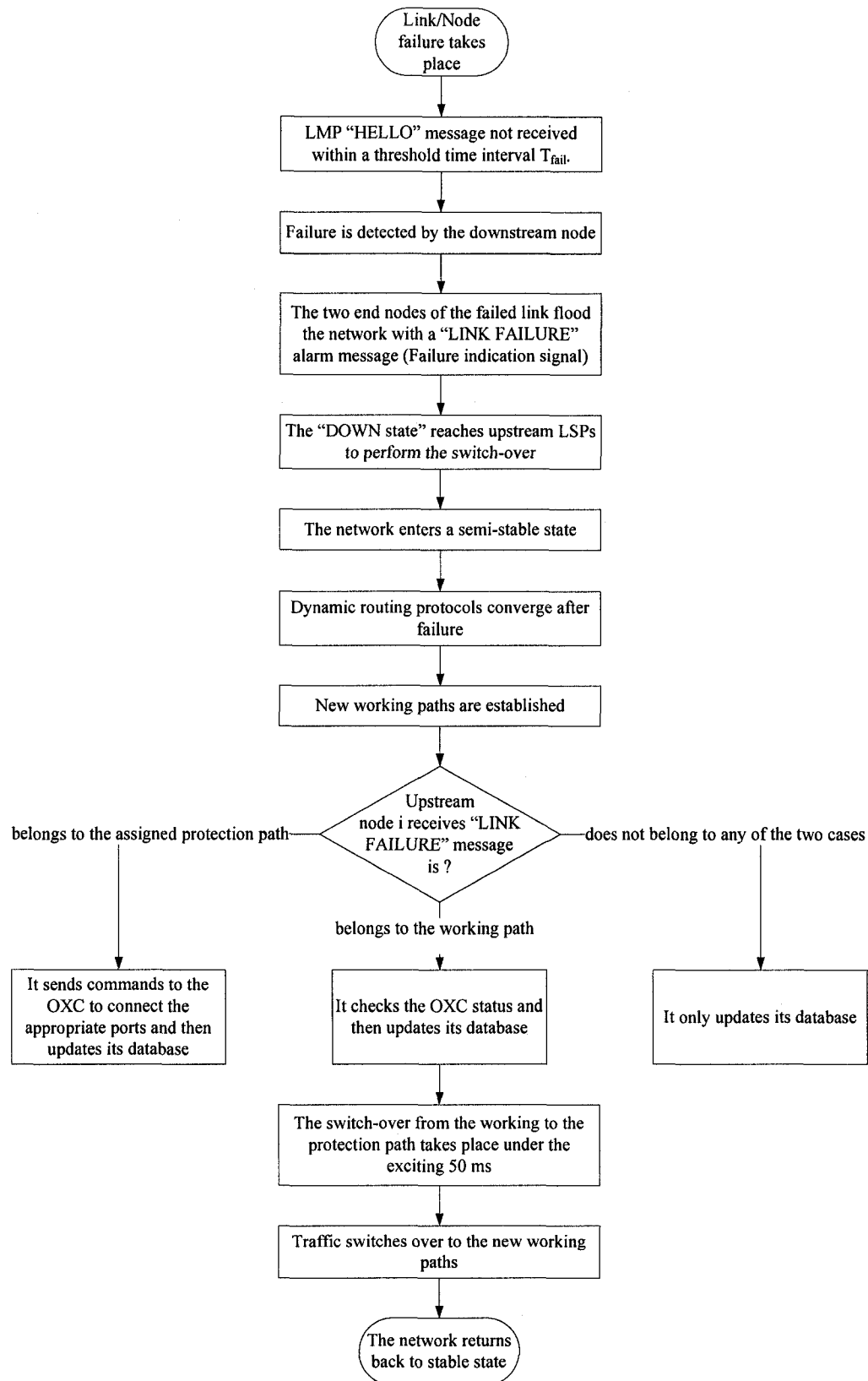


Fig. 2.24: Restoration Re-routing Process

Chapter 3: Multi-layer Survivability Solutions

The first solution that will often cross a person's mind is to select a single survivability scheme for a certain network layer. A simple and expensive example of this is protecting the entire network by a survivability scheme from the physical layer. The comparatively long detection time of the IP layer will not introduce any interworking problem with the fast physical layer recovery [DEM99].

This choice has many drawbacks, however. Some of them are as follows:

- It is difficult to satisfy the different services transported by the network;
- It is even more difficult to do so when these services have QoS requirements;
- It can be inappropriate if the network consists of different groups of sub-networks with different services and topologies (e.g. a mixture of SONET, ATM, mesh, token-ring, etc.).

A sophisticated solution based on the above mentioned drawbacks is to differentiate between the traffic types (e.g. real time, best-effort., etc.) and use different survivability classes in the physical layer. The higher survivability class is assigned to the higher CoS. The different classes are then mapped into different paths of the server layer. Obviously, this solution requires a protection scheme with a determined level of selectivity, and would have to be very sophisticated in its design.

The second solution, which makes a great deal more sense, is to adapt the multi-layer survivability concept. This involves selecting two (or more) single-layer survivability schemes from different layers and making use of their complementary characteristics.

The third solution involves combining a fast protection scheme in a server layer with the slower IP restoration. This can be a good choice for guarantee a certain QoS to real time services. By following this approach, however, the network design becomes more complex and services costs are expected to increase. The trade-off between service level QoS and the service cost is thus a challenging issue here.

Although multi-layer survivability looks like the most promising solution for survivability in multi-service environments, its problems relating to the use of different survivability schemes from different layers need to be resolved before it can be adopted. Some of those problems are the following:

- Unwanted possible interaction between the different survivability schemes when they handle alarm messages and propagate control signals;
- One or more unnecessary protection actions as a result of a single failure may trigger multiple recovery schemes (since the detection time is generally smaller than the overall restoration time.)

The results and consequences of these problems in the network can be summarized as any combination of the following:

- Extended down-time;
- The network left in an unknown state;
- Increased complexity of maintenance procedures.

3.1. Survivability Strategies

There are certain strategies that can be used to overcome the above mentioned problems:

1. Appropriate selection of survivability schemes;
2. Use of a hold-off time concept;
3. Layer escalation;
4. Sub-network escalation;
5. Scheme escalation;
6. Inter-layer signaling; and
7. Management integration.

A closer look at these solutions gives more details about their principles:

- The first strategy requires the minimum redesign of the network management,
- For the second to the fifth strategies, more protocols have to be involved to handle these scenarios,
- The first to the fifth generally neither involve any interaction between the network layers nor use any signaling for which the network management is responsible. However, they may make use of the integration between the network management and between the client and the server layer.
- The last two strategies require more interaction between the network layers, which is achieved by signaling and thus involves the network management.

3.1.1. Appropriate Selection of Survivability Schemes

In some cases, one survivability scheme from a network layer is selected to perform the survivability of the entire network [DEM99].

According to the problem stated before, the selection of a scheme is very difficult and subject to a trade-off between the network performance and its cost.

The factors that may help the network designers in making the decision include

- Topology,
- Design,
- Size, and
- Service.

The selected survivability scheme has to get the maximum out of the combined performance measures, such as detection time, coverage, restoration time, complexity, etc.

3.1.2. Hold-off Time

Deploying the hold-off time concept in the multilayer network survivability may be a solution for the layers that have a fast detection time.

The time period after failure detection forces the upper layers' restoration schemes to wait and not to take any action until either

1. The hold-off time expires, or
2. The restoration is completed by the lower layer.

If the hold-off time expires before the restoration is performed, the survivability scheme of the higher layer will come into effect.

At present, the concept of hold-off time is standardized in SONETs only to solve the conflict problem between an automatic protection scheme working at the path layer (both lower and higher orders) and an automatic protection scheme working at the line layer. The most used schemes in SONETs are SNCP and Trail Protection for the individual optical lines. The hold-off time is adjustable from 0 to 10 seconds in 100 ms steps.

It is not necessary for the fault status signal to be present for the entire duration of the hold-off time period; it is required only at its expiry. Also, the fault notification signal that triggers the hold-off timer does not have to be the same one that occurs at the expiry of the hold-off period.

The only disadvantage of using the hold-off time strategy, which also causes some degradation in the protection speed, can occur when the higher layer survivability scheme is the appropriate scheme but it cannot be employed first since it has to wait until the lower layer's survivability scheme fails. However, in some typical applications this degradation is frequently neglected.

The concept of hold-off time, although it is designed for SONET services, is also promising for other services like ATM and OTN. There has been some recent research on this point, but the concept has not yet been standardized. Also, the concept of hold-off time is difficult to implement in a multi-vendor environment because of the deficiency of standards.

3.1.3. Inter-layer Signaling

Another approach to improving the performance of survivability and solving the multi-layer survivability problems is to use real-time signaling between layers for information exchange and thus allowing the inhibition of a protection action in one layer when another layer is already engaged in protecting the same fault.

A number of OAM signals are currently used within each network layer (intra-layer OAM) mostly for fault localization and performance monitoring, while only a simple maintenance signal has been developed at the present time. This signal is the Alarm Indication Signal (AIS). It is transmitted from the server layer to the client layer to do

simple fault localization, and does not disseminate any information to the client layer about the protection action that may be in progress at the server layer.

Having more detailed status information about the server layer is beneficial to the client layer, as the latter can make use of it. An example to this is in the 1+1 OCh protection scheme when a failure affects the protecting channel. This information does not need to be forwarded to the client layer because it does not directly affect the service. On the other hand, this information will allow the client layer to react more efficiently when a failure affects the protected (working) channel.

Defining a set of OAM inter-layer signals is not an easy task, as the service layer is designed to support a variety of different clients. Nevertheless, this approach is considered to be very promising.

Another approach allows for real time co-ordination between the IP and the optical layer based on the MPLS concept in which the integration is done between the control plane of the MPLS LSR and the controller of the optical Network Element, typically an OXC.

3.1.4. Layer Escalation

Layer escalation is the most typical scheme. Each layer of the network has its own restoration system, and the systems interact to realize restoration. For example, restoration is tried in the lowest layer (OTN) first. If not all failures are restored, then higher layer restoration tries to eliminate them. Restoration proceeds layer by layer, starting at the lowest layer. This scheme is named bottom-up escalation [NED95A]. In order to achieve cost effectiveness, spare resources are shared between multiple layers [STR96A].

3.1.5. Sub-network Escalation

This scheme varies the restoration area. First, restoration is attempted in a restricted (small) area. However, if not all failures can be restored in that area because of a lack of backup routes or spare resources, the restoration area is expanded. For example, restoration is first tried between nodes directly connected to the failed link. If this fails, the restoration is next tried between path termination nodes. The expansion of the restoration area extends the failure into a wider area of the network, but it may also improve the restorability of the failed path [STR96A].

3.1.6. Scheme Escalation

Scheme escalation changes the restoration scheme if the first scheme cannot restore all failures. For example, the preplanned scheme is tried first, and the dynamic planned scheme is tried next if some failures remain [STR96A].

3.1.7. Management Integration

In general, every network layer has its own management that is completely independent from the others. Network administration is more difficult in the complex multi-layer service architecture (e.g. IP/ATM/SONET/OTN) than in the simplified service stacks (e.g. IP/POS/OTN, and IP/GbE/OTN).

In the multi-layer survivability scheme, the network layer management information is very important to the adjacent network layer management. An example is when OTN (OCh) (as a server layer) gets information about the required level of survivability from the IP (as a client layer). It helps to make better decisions regarding topology, routing, and types of protection. On the other hand, when being

forwarded back to the IP client layer, this information is used by OSPF to define different paths for different TOS as it translates to “link costs”. Therefore, the integrated survivability strategy will be improved by the use of inter-layer management (umbrella management).

3.2. Survivability in Different Integrated Multi-layer Network Architectures

The general principles of multi-layer survivability are applied to a number of network architectures as alternatives for the integration of IP over Optical Networks.

These architectures are:

- 1) IP/ATM/SONET/OTN (reference architecture)
- 2) IP/POS/OTN
- 3) IP/ GbE /OTN
- 4) IP-MPLS/OTN.

3.3. The IP/ATM/SONET/OTN Architecture

In the long-haul transport over OTN, SONET is currently the most standard transmission format deployed. ATM provides the backbone of many of the service providers. The IP/ATM/SONET/OTN architecture is selected as a reference. The reason for this is because it is still widely used in today’s backbone networks. Nevertheless, this architecture is not appropriate for meeting the promising requirements of backbone networks because of its complexity, duplication of functionality, cell tax, limited scalability, etc.

There are many approaches to IP over ATM:

- Classical IP over ATM (RFC 1483),
- LAN Emulation (LANE),
- Multi-protocol over ATM (MPOA).

From those encapsulation methods, the Classical IP over ATM (RFC 1483) has been selected as the model for this protocol stack.

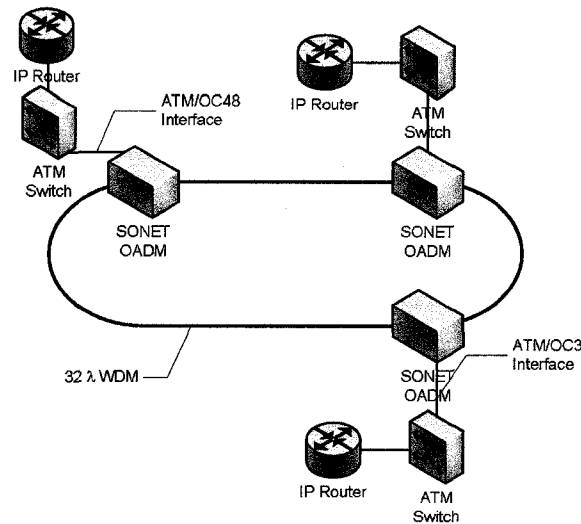


Fig. 3.1: General Example of IP over ATM over SONET Encapsulation for Transport over a OTN Network

Fig. 3.1 shows an example of the Classical IP over ATM (RFC 1483) architecture (details of this encapsulation method are described in Appendix C). Fig. 3.2 illustrates three options for ATM in SONET.

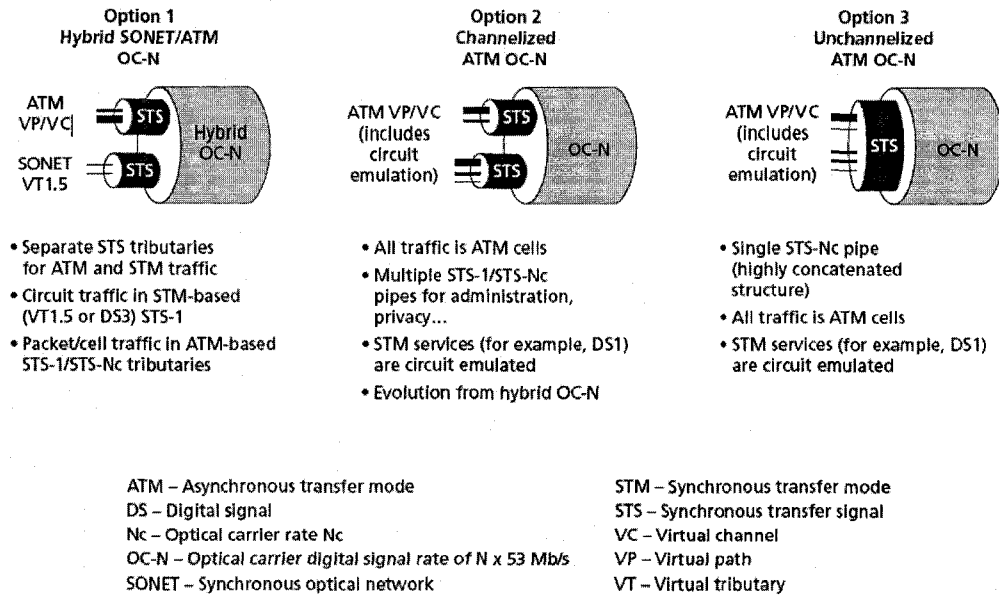


Fig. 3.2: Three Options for ATM in SONET [AND97B]

3.3.8. Available Single-layer Survivability Schemes

In the IP/ATM/SONET/OTN architecture, each one of the four layers has its own survivability schemes. Table 3.1 lists those schemes.

Table 3.1: Survivability Capabilities of the Network layers in the IP/ATM/SONET/OTN Architecture

Layer/ Sub-layer	Protection	Restoration
IP		X
ATM	X	X
SONET Path	X	X
SONET MS (Line)	X	
OTN OCh	X	X
OTN OMS	X	

The survivability mechanisms available in each of these different network layers differ mainly in terms of protection time, granularity, fault coverage, and cost.

3.3.9. Available Multi-layer Survivability

Functionality duplication is the main problem in the IP/ATM/SONET/OTN architecture.

This duplication is clear in single-layer survivability and more complex in multi-layer survivability strategies. Table 3.2 lists the available survivability schemes for the IP/ATM/SONET/OTN architecture or protocol stack.

Table 3.2: Available Multi-layer Survivability Schemes in the IP/ATM/SONET/OTN Architecture

Multilayer	Survivability Scheme used
IP(restoration)/ SONET(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ SONET(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ OTN(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ OTN(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
ATM(restoration)/ SONET(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
ATM(restoration)/ SONET(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
ATM(restoration)/ OTN(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
ATM(restoration)/ OTN(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration

The most suitable scheme that has been deployed in many existing networks is the use of a hold-off timer, while Layer Escalation and Inter-layer signaling schemes are

difficult to deploy due to the number of layers exist in this stack. The most challenging decision is whether to assign restoration or protection in a lower layer to maintain all traffic together, or to assign either restoration or protection in a higher layer to maintain traffic priorities. Thus, combining these two solutions together will produce enhanced results.

3.4. The IP/SONET (POS)/OTN Architecture

The second network architecture scenario selected is IP over SONET over OTN. In general, there are two possibilities for IP over SONET, as shown in Fig. 3.3. The first is simply to encapsulate IP packets into SONET formats and transmit them over OTN (by using a transponder). This is called POS Packet over SONET (RFC 1619, RFC 1661, and RFC 1662). The second is to encapsulate the IP packets along with other traffic into SONET formats and transmit them over OTN links. This is called SDL over SONET (RFC 2823).

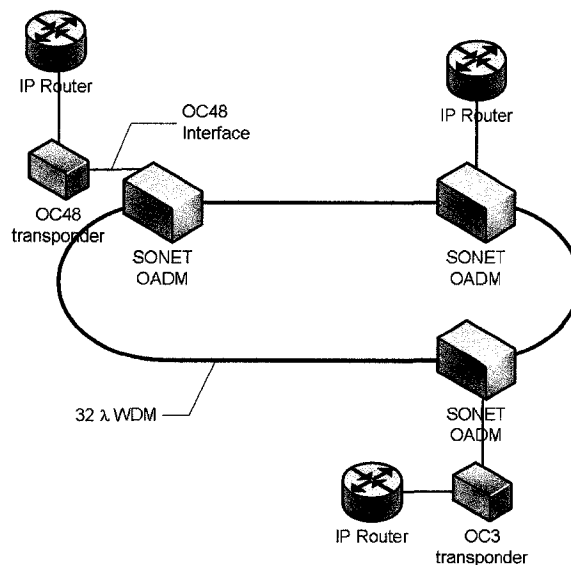


Fig. 3.3: Example of IP over SONET over OTN Network

3.4.1. Available Single-layer Survivability Schemes

The OTN layer can provide fast protection both at the OMS and at the OCh layers while restoration can be implemented in the OCh layer, only. SONET has already a wide range of protection and restoration standard schemes available; however, the only protection scheme applicable to this scenario whereas SONET is integrated in the router interfaces is the 1+1 Linear MSP (Multiplex Section Protection). This is a fast automatic protection scheme that can protect the SONET signal with a switching time lower than 50ms. The IP layer provides a robust restoration mechanism based on packet re-routing in case of failure and integrated in the routing protocols. The survivability capabilities of the three layers of the IP/POS/OTN architecture are summarized in Table 3.3.

Table 3.3: Survivability Capabilities of the Network layers in the IP/POS/OTN Architecture

Layer/ Sub-layer	Protection	Restoration
IP		X
SONET Path		
SONET MS	X	
OTN OCh	X	X
OTN OMS	X	

3.4.2. Available Multi-layer Survivability

In the IP/SONET (POS)/OTN, the problem with functionality duplication is less complicated than the IP/ATM/SONET/OTN architecture. Table 3.4 lists the available survivability schemes for the IP/SONET (POS)/OTN architecture or protocol stack. The most suitable scheme that has been deployed in many existing networks is still the use of hold-off timers, while layer escalation and inter-layer signaling schemes

are still difficult to deploy in this architecture due to the same large number of layers that exist in this stack.

Table 3.4: Available Multi-layer Survivability Schemes in the IP/SONET (POS)/OTN Architecture

Multilayer	Survivability Scheme used
IP(restoration)/ SONET(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ SONET(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ OTN(restoration)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ OTN(protection)	Hold-off timer, Sub-network Escalation, Scheme Escalation, Management Integration

Combining restoration or protection in a lower layer with either restoration or protection in a higher layer is still a good decision for enhancing the survivability results. An example of combined restoration can be applied to the network of Fig. 3.3, where the OTN ring is survived by 1+1 OCh OTN protection and IP restoration.

3.5. The IP/GbE/OTN Architecture

Of all current networking protocols, Ethernet has by far the highest number of installed ports (85% of LANs world-wide). It provides also the greatest cost performance relative to Token Ring, Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM) for desktop connectivity.

Fast Ethernet, which increases the Ethernet speed from 10 to 100 megabits per second (Mbps), provides a simple and cost-effective option for backbone and server connectivity. The new Gigabit Ethernet extends high-capacity LANs to MANs and

probably WANs. This configuration may cost 5 times less than SONET OC192 links.

Fig. 3.4 shows an example of an IP network based on Gigabit Ethernet interfaces.

It is simple to encapsulate and frame IP packets in Gigabit Ethernet. Because Gigabit Ethernet is full-duplex, the CSMA-CD functionality is not used. Ethernet switches are used to expand the network topology further than a point-to-point link. Thus, in Gigabit Ethernet over OTN, the packet level routing is done by the IP layer, while the wavelength routing is realized in the optical layer. Gigabit Ethernet provides QoS as specified in the standards IEEE 802.1Q and 802.1p, which define CoS for different IP packets. RSVP or DiffServ use these CoS to support their operations.

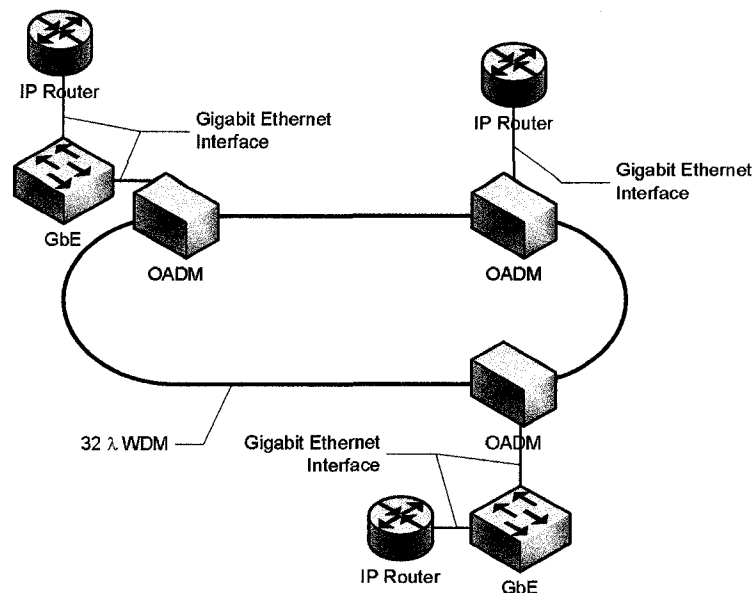


Fig. 3.4: Example of IP being transported over a OTN Ring with Gigabit Ethernet Framing

3.5.1. Available Single-layer Survivability Schemes

GbE does not provide any kind of survivability mechanisms. So, in this network architecture, the survivability is facilitated by only OTN and IP layers.

The available survivability mechanisms for this architecture are summarized in Table 3.5.

Table 3.5: Survivability Capabilities of the Network Layers in the IP/GbE/OTN Architecture

Layer	Protection	Restoration
IP		X
GbE		
OTN OCh	X	X
OTN OMS	X	

3.5.2. Available Multi-layer Survivability

As this architecture contains only two layers which have survivability functions, it can be considered not difficult to analyze. Table 3.6 lists the available survivability schemes for the IP/GbE/OTN architecture or protocol stack. The most suitable scheme that has been deployed in many existing networks is still the use of hold-off timers. All other survivability schemes can also be implemented, as there are only two layers that support survivability functions.

Table 3.6: Available Multi-layer Survivability Schemes in the IP/GbE/OTN Architecture

Multilayer	Survivability Scheme used
IP(restoration)/ OTN(restoration)	Hold-off timer, Layer Escalation, Inter-layer signaling, Sub-network Escalation, Scheme Escalation, Management Integration
IP(restoration)/ OTN(protection)	Hold-off timer, Layer Escalation, Inter-layer signaling, Sub-network Escalation, Scheme Escalation, Management Integration

Combining restoration or protection in a lower layer with either restoration or protection in a higher layer is also a good option for enhancing the survivability results.

3.6. IP-MPLS/OTN Architecture

Multi-Protocol Label Switching (MPLS) is a tunneling technology used in many service provider networks. An IP core merges the separate control planes of two-layer and three-layer networks into a single entity. This integration eliminates the management burden of coordinating the operation of two distinct networks, and also permits routing and automated traffic engineering to occur on the same platform in order to reduce the operational cost of the network. Furthermore, an IP core that supports MPLS offers numerous advantages by using traffic engineering to maximize the efficient use of bandwidth and reduce congestion [YIN01].

3.6.1. Available Single-layer Survivability Schemes

MPLS supports much finer and more flexible bandwidth granularity than re-configurable OTN (per LSP versus per wavelength). This means that MPLS requires less spare capacity. Moreover, MPLS can make service differentiation between flows identified by LSPs, carried on a single wavelength [ZHA02]. Therefore, one can choose to protect those LSPs, only, that have stringent QoS requirements. The available survivability mechanisms for this architecture are summarized in Table 3.7.

Table 3.7: Survivability Capabilities of the Network Layers in the IP-MPLS/OTN Architecture

Layer	Protection	Restoration
IP-MPLS	X	X
OTN OCh	X	X
OTN OMS	X	

3.6.2. Available Multi-layer Survivability

This architecture not only contains two layers which have survivability functions, but also these functions can be integrated together with MPLS control management. Table 3.8 lists the available survivability schemes for the IP-MPLS/OTN architecture or protocol stack. The most suitable scheme in this architecture to be implemented is Management Integration. Combining restoration or protection in a lower layer with either restoration or protection in a higher layer is a good choice for enhancing the survivability results.

Table 3.8: Available Multi-layer Survivability Schemes in the IP-MPLS/OTN Architecture

Multilayer	Survivability Scheme used
IP-MPLS(restoration)/ OTN(restoration)	Hold-off timer, Layer Escalation, Inter-layer signaling, Sub-network Escalation, Scheme Escalation, Management Integration
IP-MPLS(restoration)/ OTN(protection)	Hold-off timer, Layer Escalation, Inter-layer signaling, Sub-network Escalation, Scheme Escalation, Management Integration
IP-MPLS(protection/ restoration)/ OTN(protection)	Hold-off timer, Layer Escalation, Inter-layer signaling, Sub-network Escalation, Scheme Escalation, Management Integration

Chapter 4: Performance Evaluation

For evaluation of the proposed multi-layer survivability strategies and interworking mechanisms, a simulation platform was developed based on Matlab. Each experiment was carried out several times to get accurate results with a 95% level of confidence. A single link failure scenario is assumed, which is the most probable type of failure to occur in networks.

4.1. Network Architecture Model used

The simulation is carried on a backbone network of 8 nodes and 13 links (Fig. 4.1), leading to an average nodal degree of 3. Each node aggregates traffic from at least 10 subnets, and in the topology it consists of an OXC and an attached IP router. The nodes are connected by a single two-fiber cable carrying 64 wavelengths, and each wavelength is OC-192 (9.952 Gb/s).

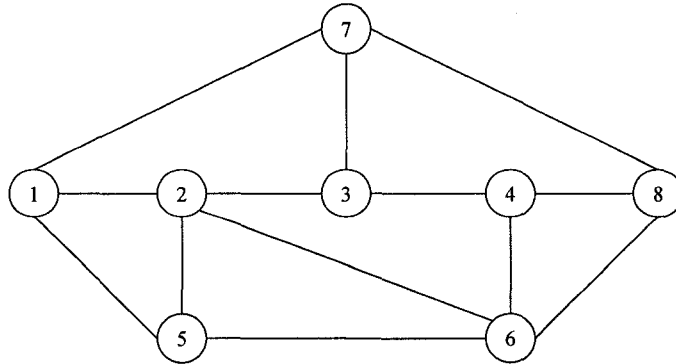


Fig. 4.1: Network Architecture Model used in the Simulation

4.1.1. Network Traffic

The network traffic is generated in terms of connection requests. A connection request is a demand to establish a lightpath from a source node to a randomly chosen destination node. The connection requests arriving at each node are assumed to follow the Poisson process with a mean ranging from 1-80 connections/s, and the holding time will be exponentially distributed with a mean of 30 minutes. Each request's source node and destination node are selected based on uniform distribution. The connection requests are randomly assigned capacity that varies between OC-1 and OC-192. If it happens that a same source to a same destination is requested, either the node does traffic aggregation, while the total capacity is below OC-192, or it launches a new wavelength.

4.1.1.1. Network Traffic Process

Studies of high-resolution traffic measurement from different working communication networks have provided ample evidence that actual network traffic in the Internet is self-similar or fractal in nature [GHO05]. Network arrivals are often modeled as Poisson process for analytic simplicity, even though a number of traffic studies have shown that packet inter-arrivals are not exponentially distributed. User-initiated TCP session arrivals, such as remote-login and file-transfer, are well-modeled as Poisson process with fixed hourly rates, but other connection arrivals deviate considerably from Poisson. However, modeling TELNET packet inter-arrivals as exponential distribution grossly underestimates the burstiness of TELNET traffic, but using the empirical TcpIib inter-arrivals preserves burstiness over many time scales. On the other hand, FTP data connection arrivals within FTP sessions

come bunched into large “connection bursts,” which are so large that they completely dominate FTP data traffic [PAX05].

However, in the simulation, we used Poisson process for ease of analysis, for Matlab support, and because of our focus on the transport layers survivability performance which does not depend on the traffic behavior.

4.1.2. Routing and Wavelength Assignment RWA

In order to compute an explicit route, it is much easier to use a link state-based routing algorithm. Indeed, the lightpath to be established will be more optimal if each node has a complete knowledge of the network. It is also a property of the Dijkstra algorithm that the complete route from the source to any other node in the network can be easily found by performing recursive iteration on the graph. This makes it very easy to use the Dijkstra algorithm in order to find an explicit route. In link state-based routing, information is only sent when changes occur. A node first builds up a description of the topology of the network. Then it may use any routing algorithm to determine the route.

A wavelength assignment algorithm is used to pre-configure backup lightpaths. Using traditional routing protocols, all the traffic follows the shortest path.

4.1.3. Wavelength Converters

It is assumed that wavelength converters are deployed at all network nodes in most of the simulations, and that there is no wavelength continuity constraint. The number of wavelength converters is sufficient in order not to have traffic blocking at/inside any node in the network.

4.1.4. Load Balancing

It is also assumed that a network design has planned optimal bandwidth allocation and traffic loading, so the traffic load is distributed in the network links.

4.1.5. Network Management

All nodes communicate via a centralized control plane that controls all the survivability functions either in single- or multi-layer survivability according to the different architectures proposed.

4.2. System Parameters

The system parameters can be grouped into three categories:

- 1) Fixed parameters; which are typical network performance either taken from practical implemented networks or as an outcome of a simulation. Table 4.1 lists these parameters [FUM00] [AUT98] [QIN03],
- 2) Variable parameter; where the simulation takes care of it, e.g., the total number of wavelengths deployed on each link, the call arrival time and the call hold time,
- 3) The performance parameter; which is the time taken from the failed link to return back to its average traffic after recovery. The average traffic the network sustained at the equilibrium for the link under consideration is taken as a reference to be compared with the traffic after recovery.

Table 4.1: Simulation Network Parameters

OTN	Average Detection Time	0.125 ms
	Virtual Wavelength Path switching time	20 ms
	Per - node processing delay	3 ms
	OXC connection matrix reconfiguration time	25 ms
	Hold-off timer	150 ms
	Link propagation delay	0.3 km/ μ s
	OCh and OMS Restoration completion time	50 ms
ATM	Detection	0.1ms
	VP switching time	0.1 ms
	ATM hold-off time	50 ms
	ATM OAM signal processing	10 ms
	ATM routing table reconfiguration time	30 ms
IP	Detection	1s
	IP dynamic routing (Detection time)	100 ms–180 s
	IP dynamic routing (Restoration completion time)	1–100 s
	Routers processing delay (approximately)	0.2 ms.
MPLS	MPLS fast (link) rerouting (Detection time)	0.1–100 ms
	MPLS fast (link) rerouting (Restoration completion time)	50–100 ms
	MPLS edge-to-edge rerouting (Detection time)	100 ms–180 s
	MPLS edge-to-edge rerouting (Restoration completion time)	1–100 s
	LSR forwarding table reconfiguration time	50 ms
SONET	Detection	3 ms
	Processing delay	$0.375 + N \times 0.25$ ms
	SONET path switching time	20 ms
	SONET switching matrix reconfiguration time	25 ms

4.3. Simulated Survivability Schemes

In our simulation, we use the survivability schemes done at the Information and Telecommunication Technology Center (ITTC), University of Kansas, for the Service Independent Access Point (SIAP) project.

4.3.1. OTN Restoration

Restoration time (in milliseconds) is given by:

$$t_r^{OTN} = t_{frame} + \frac{N_w l}{2 \times 10^2} + (N_w \times t_{proc}^{OTN}) + (t_{sw}^{OTN} \times S_T \times D_{aw}) \dots \dots \dots (4.1)$$

where :

$$t_{frame} = 125 \mu s$$

N_w = number of nodes to be informed of failure

l = avg. inter - node distance in km

t_{proc}^{OTN} = per - node processing delay $\approx 3ms$

t_{sw}^{OTN} = OCh switching time $\approx 20ms$

D_{aw} = affected number of OCh's

4.3.2. SONET Restoration

Restoration time (in milliseconds) is given by:

$$t_r^{SONET} = t_{det}^{SONET} + \frac{N_s l}{2 \times 10^2} + (3 \times t_{proc}^{SONET}) + (t_{proc}^{SONET} \times S_T \times D_{as}) \dots \dots \dots (4.2)$$

where :

$$t_{det}^{SONET} \approx 3ms$$

N_s = number of nodes to be informed of failure

l = avg. inter - node distance in km

t_{proc}^{SONET} = processing delay = $0.375 + (N_s \times 0.250) ms$

t_{proc}^{SONET} = SONET path switching time $\approx 20ms$

D_{aw} = affected number of SONET paths

4.3.3. ATM Restoration

Restoration time (in milliseconds) is given by:

$$t_r^{ATM} = t_{det}^{ATM} + \frac{N_a l}{2 \times 10^2} + (N_a \times t_{proc}^{ATM}) + (t_{VP} \times s_T \times D_{aa}) \dots \dots \dots (4.3)$$

where :

$$t_{det}^{ATM} \approx 0.1ms$$

N_a = number of nodes to be informed of failure

l = avg. inter - node distance in km

t_{proc}^{ATM} = per - node processing delay $\approx 1ms$

t_{VP} = VP switching time $\approx 0.1ms$

D_{aa} = affected number of VPs

4.3.4. IP Restoration

Restoration time (in milliseconds) is given by:

$$t_r^{IP} = 1000 + \frac{N_i l}{2 \times 10^2} + (N_i \times 3) + (12 \times s_T \times D_{ai}) \dots \dots \dots (4.4)$$

where :

N_i = number of nodes to be informed of failure

l = avg. inter - node distance in km

D_{ai} = affected number of routes

4.4. Simulation Results

4.4.1. Single-layer Survivability; IP Restoration

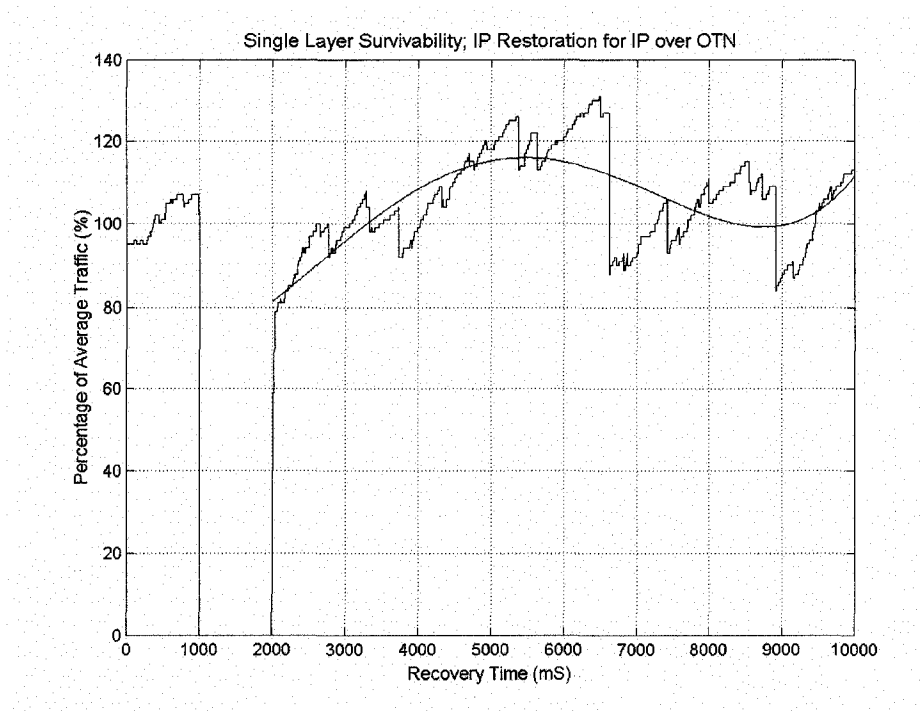


Fig. 4.2: Single-layer Survivability; IP Restoration

The IP restoration mechanism is simulated as illustrated in Fig. 4.2. It is noticed that

- The IP detection time considered here is 1s;
- The traffic reached 78% of the network average traffic after approximately 40 ms from the start of the restoration process (more details are shown in Fig. 4.3);
- The traffic restored at this point is the majority among this percentage;
- The IP transport protocols are greedy, which explains the fast restoration process;
- The centralized network management increases the weight on this link as the traffic increases;

- The use of link-state algorithms (Dijkstra) acts as a feedback in order to have the network load balance we desire;
- The IP restoration process, according to this scenario, takes an average of 8 seconds to be completed, which is close to the result claimed by the actual measurements for a real working network;
- As the IP is the server and the client in the same time, there are no difficulties in restoring all types of traffic (native traffic). The performance will indeed be different in cases when we have other clients than IP.

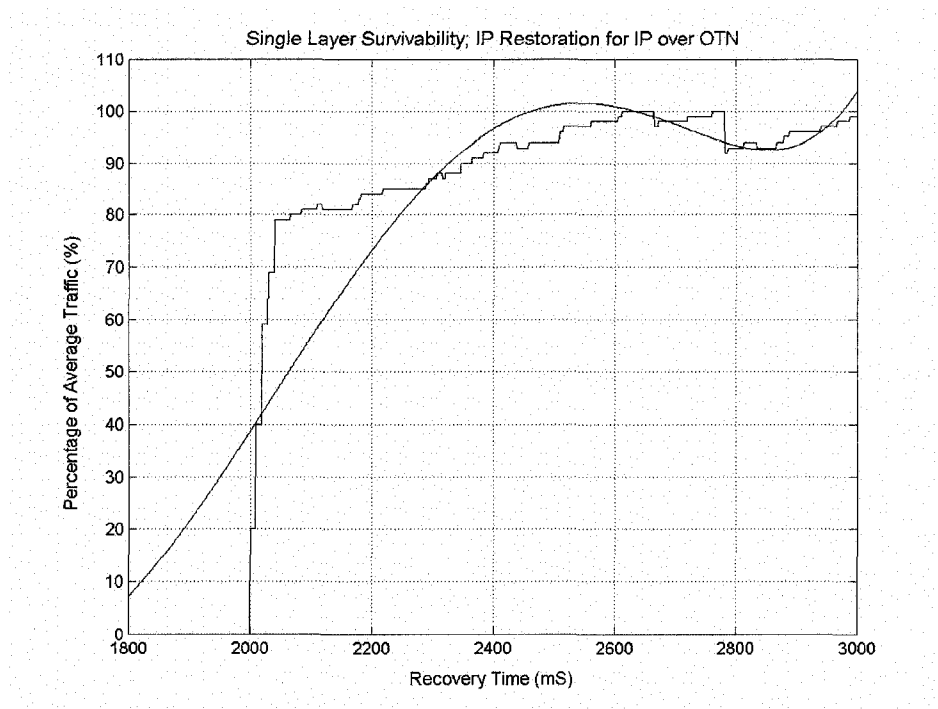


Fig. 4.3: Single-layer Survivability; IP Restoration (after recovery view)

4.4.2. Single-layer Survivability; ATM Restoration

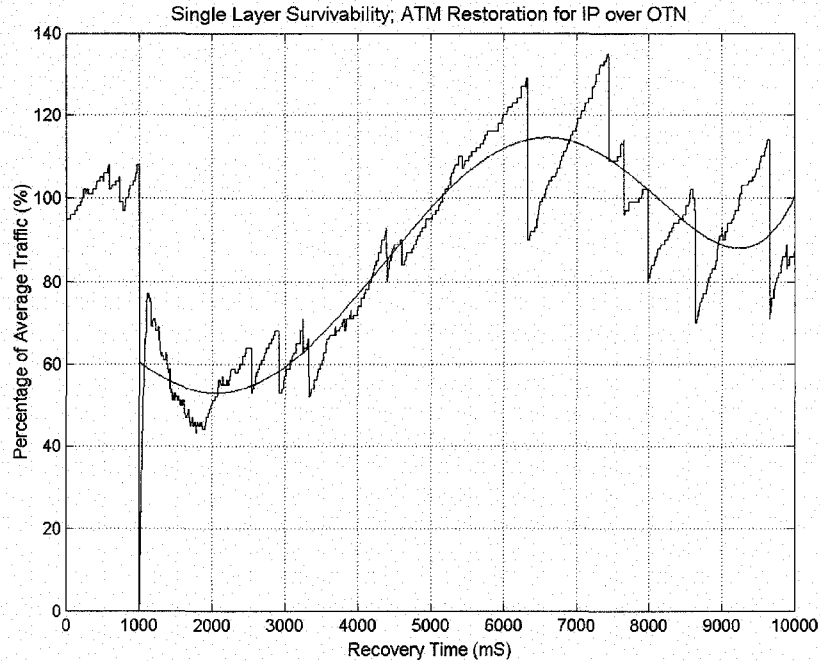


Fig. 4.4: Single-layer Survivability; ATM Restoration (complete view)

The simulation performance of the ATM restoration is shown in Fig. 4.4. The strange behavior is due to the two-step restoration process of the ATM; the rapid restoration happens because the ATM uses the routing table that existed before the fault occurrence and then performs network optimization. The VP planner unit calculates an optimal VP assignment for the latest network topology and VPs are changed accordingly (network wide restoration). The later step causes some delay, which prevents the restoration process from continuing with the same speed. It should also be noted also that the fault detection by the ATM is very fast and even better than the fault detection by the physical sub-layer of the OTN.

A focus on the start of the ATM restoration process is shown in Fig. 4.5.

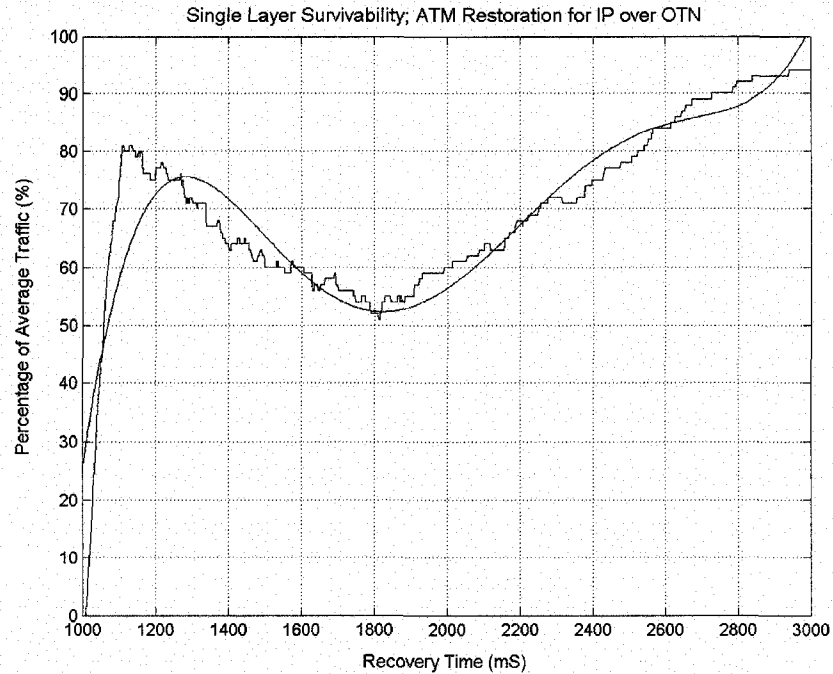


Fig. 4.5: Single-layer Survivability; ATM Restoration (after recovery view)

4.4.3. Single-layer Survivability; SONET Restoration

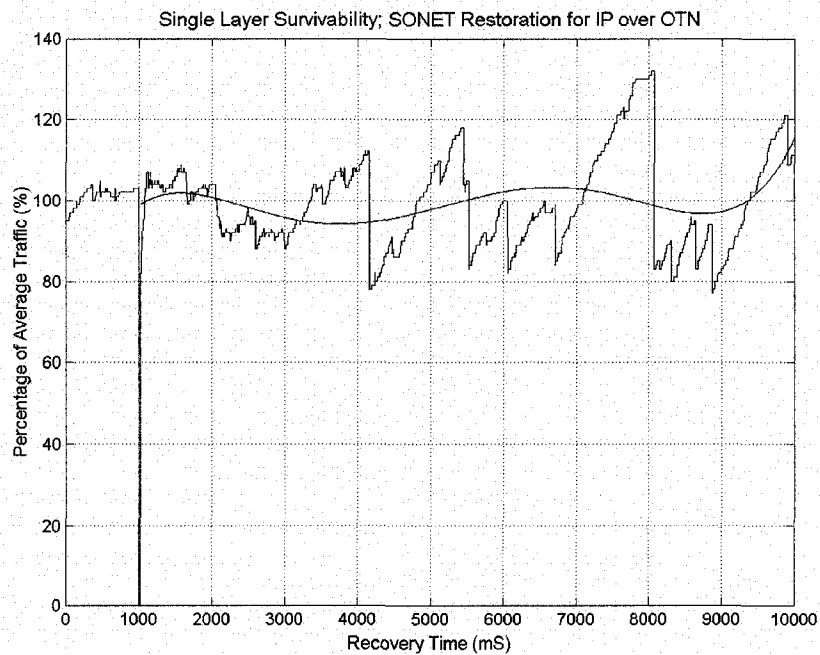


Fig. 4.6: Single-layer Survivability; SONET Restoration (complete view)

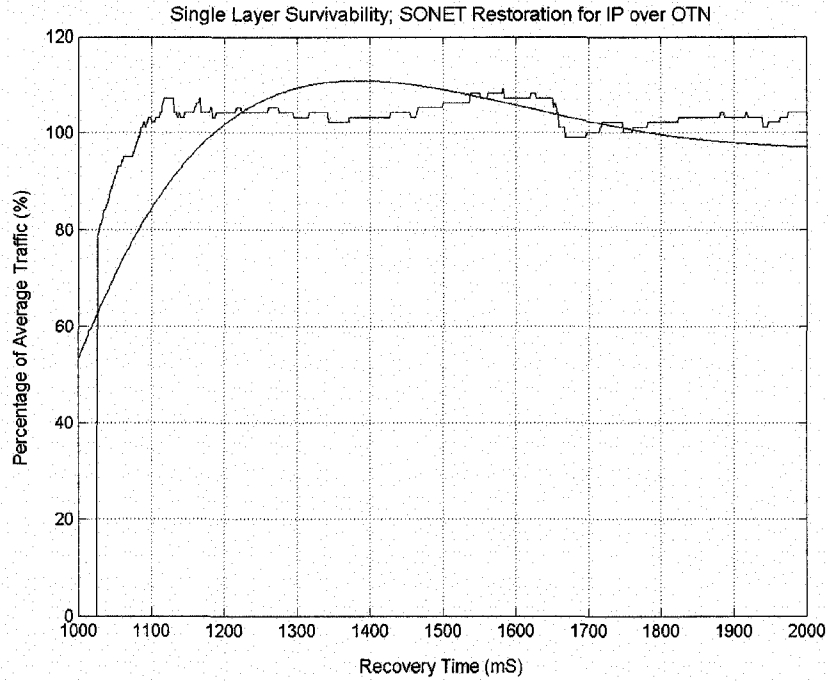


Fig. 4.7: Single-layer Survivability; SONET Restoration (after recovery view)

The SONET restoration's simulation performance is illustrated in Fig. 4.6 and Fig. 4.7 with the following remarks:

- The SONET restoration process with its ideal performance reflects its popularity in the network design and operation communities;
- Although the SONET detection time is not as fast as the ATM, its switching matrix reconfiguration time is much better than the other transport layers;
- The SONET restoration process, according to this scenario, takes less than 80 milliseconds on average to be completed, which is close to the result claimed by actual measurements of a real working network;
- As soon as the switching matrix is configured, the SONET restores the traffic, which reaches approximately 78% from the total affected traffic.

4.4.4. Single-layer Survivability; OTN Restoration

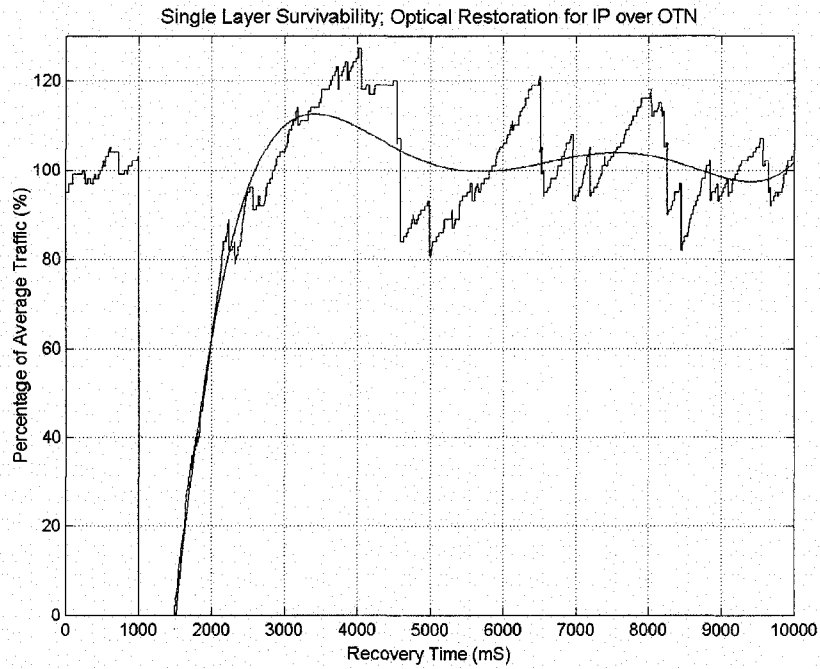


Fig. 4.8: Single-layer Survivability; OTN Restoration (complete view)

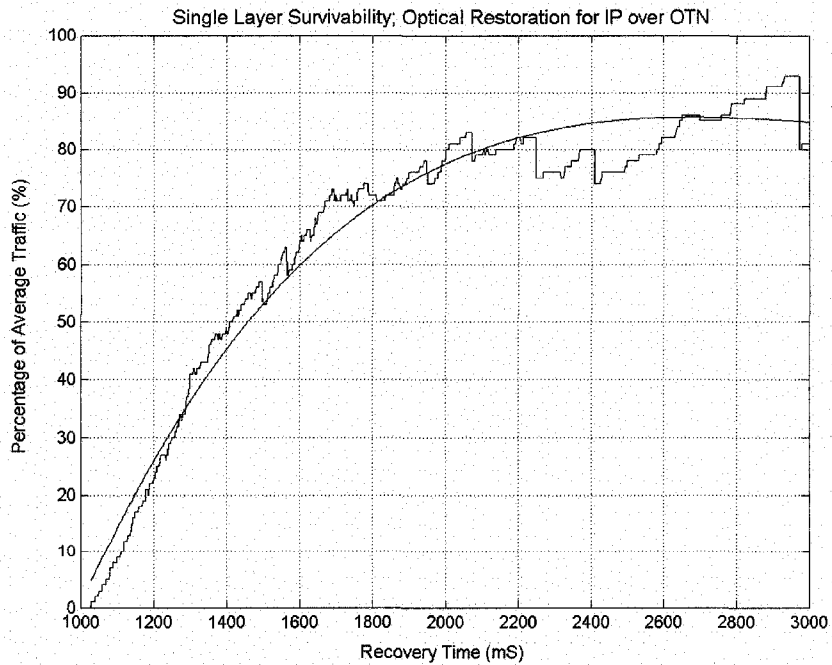


Fig. 4.9: Single-layer Survivability; OTN Restoration (after recovery view)

The OTN restoration simulation performance is illustrated in Fig. 4.8 and Fig. 4.9 with the following remarks:

- Although OTN restoration functionality looks similar to those of the SONET, its simulation performance shows some differences in performance;
- This difference is related to the SONET node processing delay which is fixed and equals 3ms on average, while in the OTN there is another factor used in calculating the restoration time for every restored optical path;
- The number of nodes to be informed about the failure is that factor which varies from one affected optical path to another.

4.4.5. Multi-layer Survivability; ATM/SONET Restoration

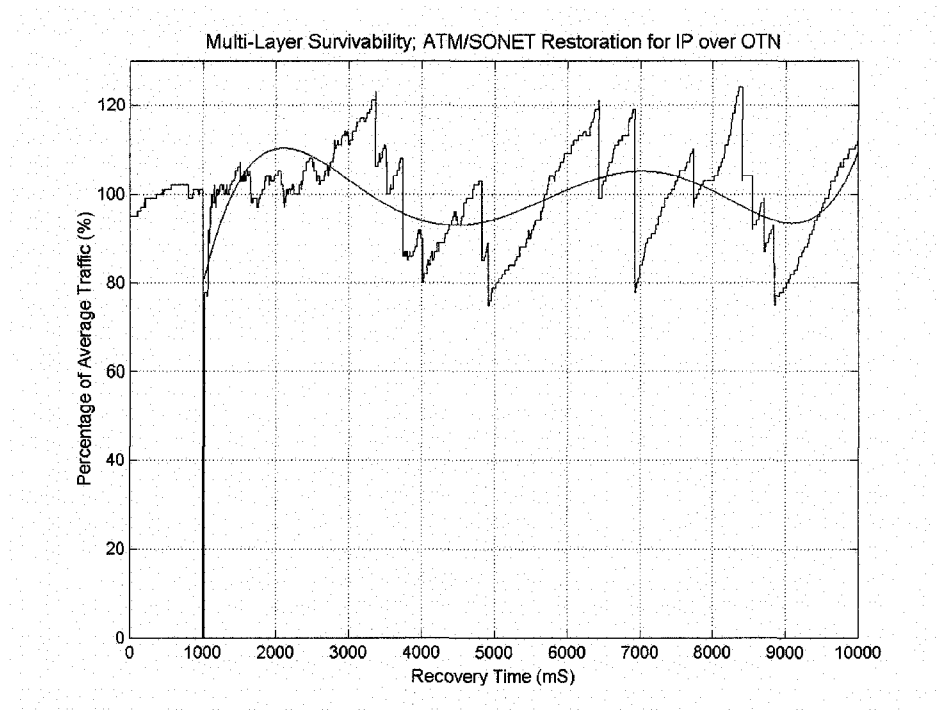


Fig. 4.10: Multi-layer Survivability; ATM/SONET Restoration (complete view)

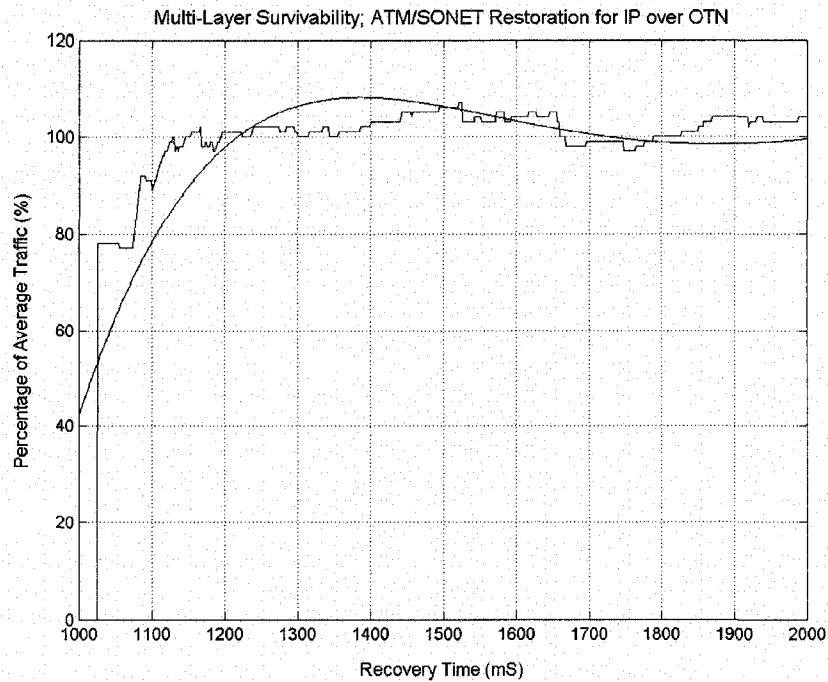


Fig. 4.11: Multi-layer Survivability; ATM/SONET Restoration (after recovery view)

The ATM/SONET multi-layer restoration simulation performance is shown in Fig. 4.10 and Fig. 4.11 with the following remarks:

- The concept of hold-off timers is considered in this scheme for a value of 50ms;
- It is noted that there are no drawbacks from implementing this scheme as the IP is the only client in the network under discussion;
- The hold-off time is sufficient for the SONET to configure the switching matrix and to restores approximately 78% of the total affected traffic;
- The disadvantage of the ATM two-step restoration mechanism does not appear clearly here as the amount of traffic left after SONET restoration is not large enough to be noticed.

4.4.6. Multi-layer Survivability; IP/SONET Restoration

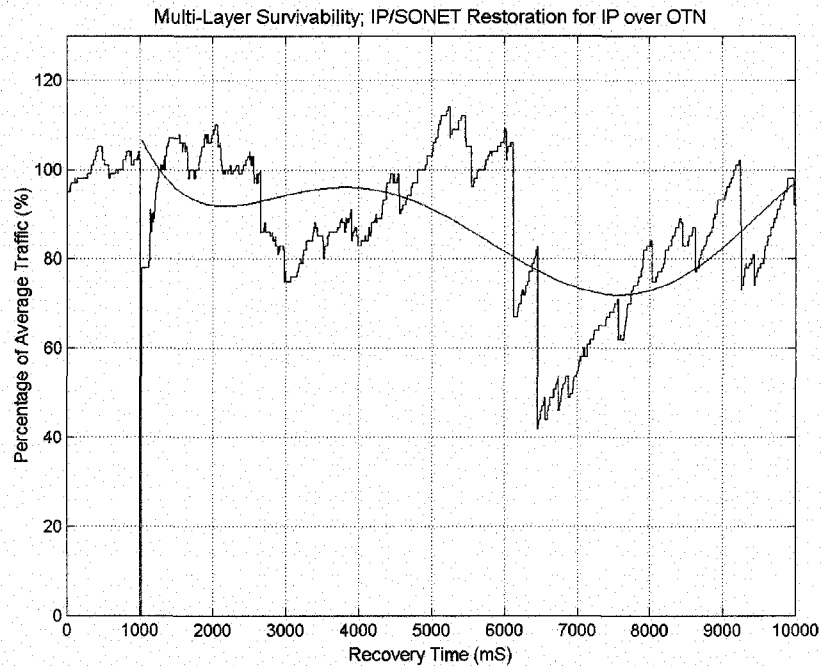


Fig. 4.12: Multi-layer Survivability; IP/SONET Restoration (complete view)

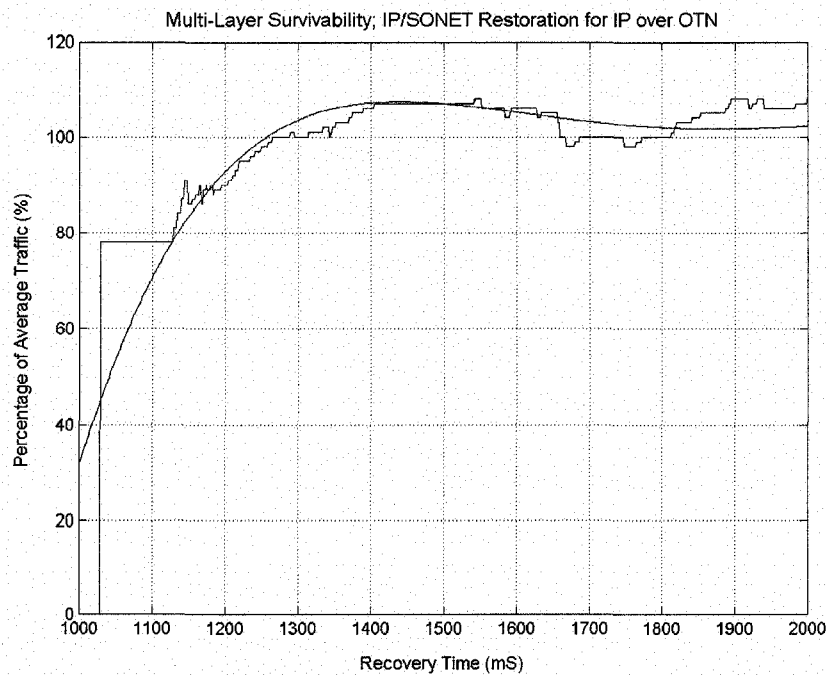


Fig. 4.13: Multi-layer Survivability; IP/SONET Restoration (after recovery view)

The IP/SONET multi-layer restoration simulation performance is shown in Fig. 4.12 and Fig. 4.13 with the following remarks:

- The concept of hold-off timers is considered in this scheme for a value of 100ms;
- The hold-off time is sufficient for the SONET to configure the switching matrix and to restore approximately 78% of the total affected traffic;
- The IP is the only client in the network under discussion;
- The layer separation between the IP and SONET and their different non-contradicting restoration functions make the integration optimal.

4.4.7. Multi-layer Survivability; IP/OTN Restoration

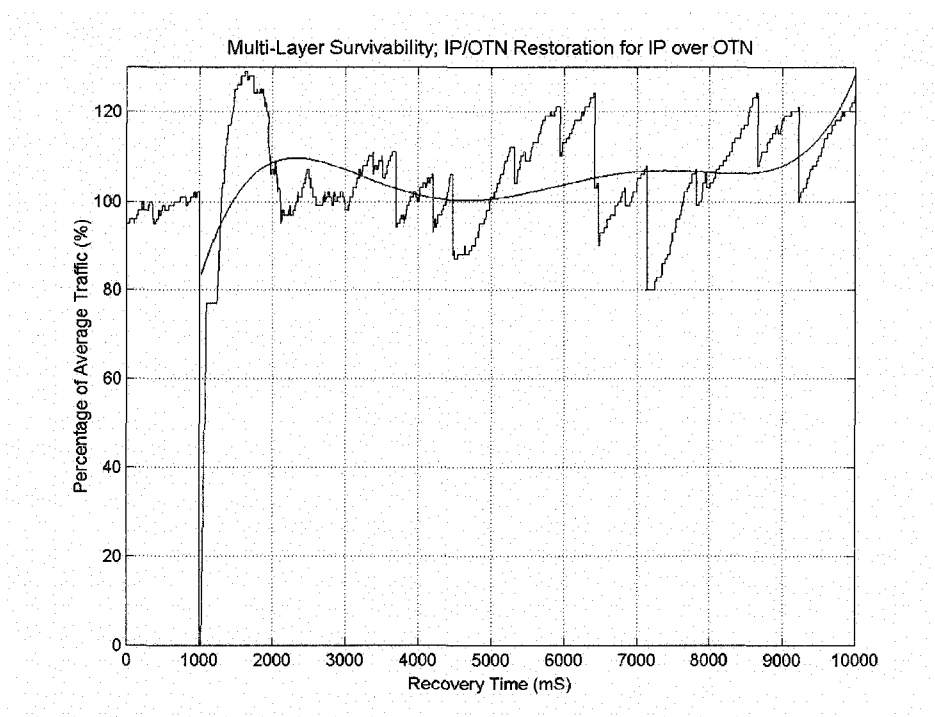


Fig. 4.14: Multi-layer Survivability; IP/OTN Restoration (complete view)

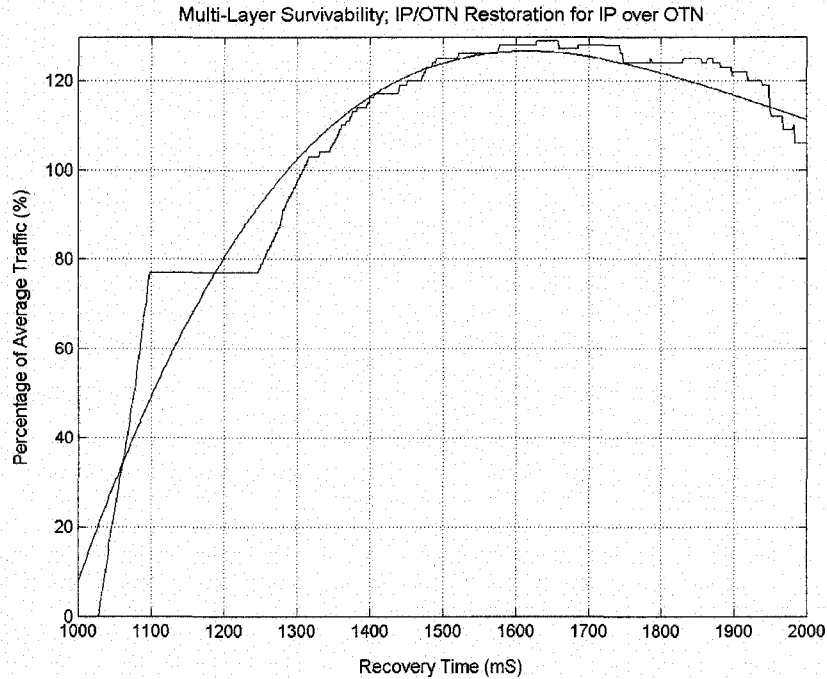


Fig. 4.15: Multi-layer Survivability; IP/OTN Restoration (after recovery view)

The IP/OTN multi-layer restoration simulation performance is shown in Fig. 4.14 and Fig. 4.15 with the following remarks:

- The concept of hold-off timers is considered in this scheme for a value of 150ms;
- The hold-off time is also sufficient for the OTN (as in SONET) to configure the Virtual Wavelength Path switching matrix and to restore approximately 78% of the total affected traffic;
- The IP is the only client in the network under discussion;
- Although the layer separation between the IP and OTN is more than IP/SONET scheme, their different restoration functions need an intelligent control plane to integrate them together (e.g. MPLS control plane).

4.4.8. Multi-layer Survivability; IP-MPLS/OTN Restoration

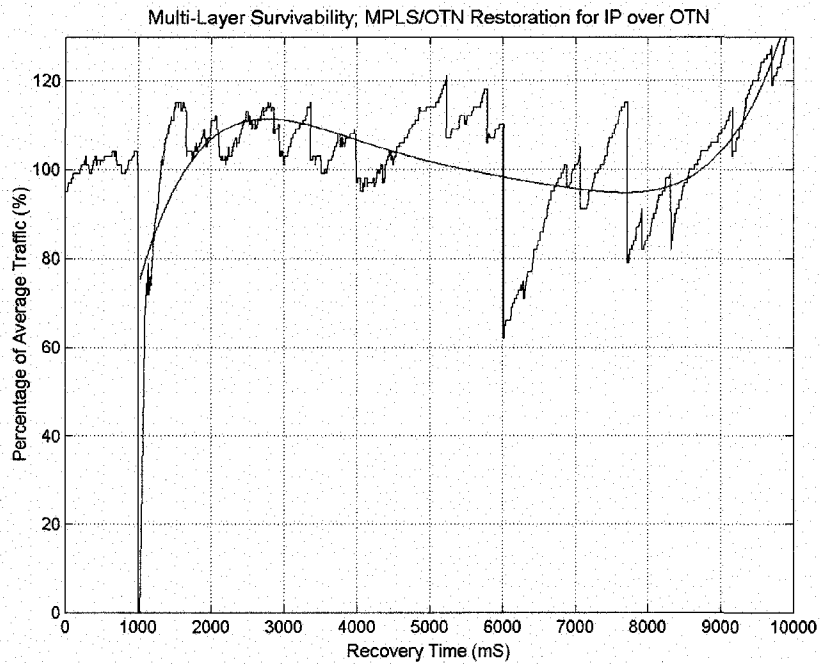


Fig. 4.16: Multi-layer Survivability; MPLS/OTN Restoration (complete view)

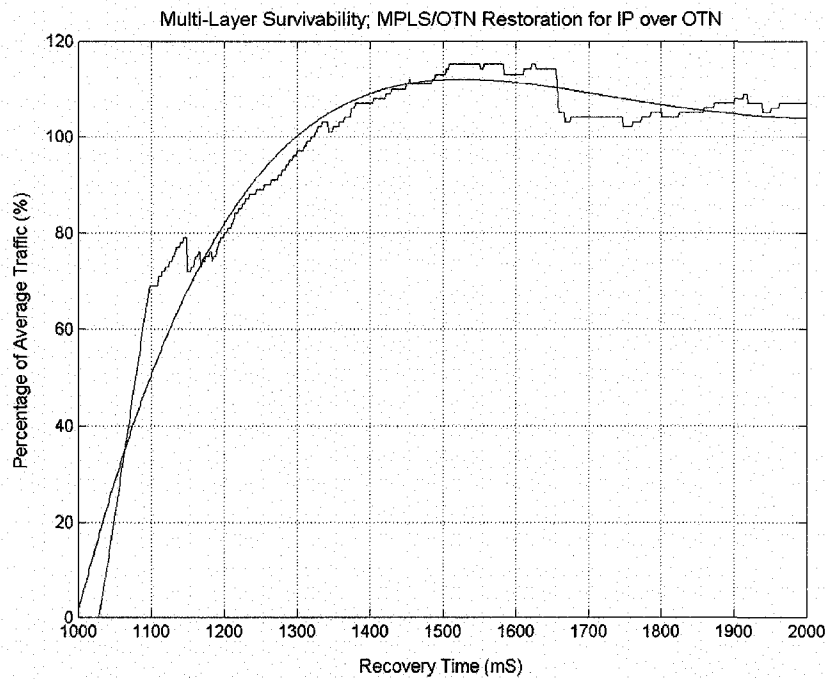


Fig. 4.17: Multi-layer Survivability; MPLS/OTN Restoration (post recovery view)

The IP-MPLS/OTN multi-layer restoration simulation performance is shown in Fig. 4.16 and Fig. 4.17 with the following remarks:

- The concept of hold-off timers is not considered in this scheme whereas the concept of management integration is used instead;
- The collaborating restoration function efforts and their integration unifies the scheme performance;
- The IP is the only client in the network under discussion.

4.4.9. Combined Multi-layer Survivability; IP - Restoration/OTN Protection

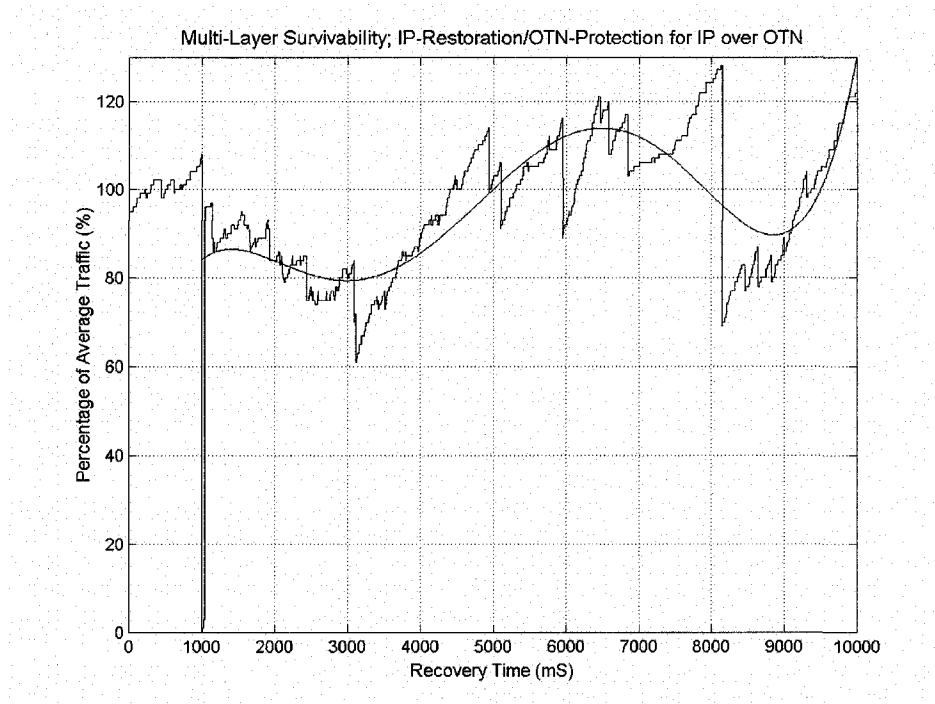


Fig. 4.18: Combined Multi-layer Survivability; IP Restoration/OTN Protection

The IP restoration/OTN protection combined multi-layer restoration simulation performance is shown in Fig. 4.18 and Fig. 4.19 with the following remarks:

- The IP is the only client in the network under discussion;

- The predicted survivability scheme demonstrates an enhancement in the outcome performance;
- Approximately 93% of the total affected traffic is restored immediately after the recovery process starts;
- Fault detection and processing take approximately 20ms, which is a part of repair time,
- The 1+1 OCh protection concept is deployed in the simulation and provides zero time switching between the working and protecting paths (we neglect the processing time taken from the management control plane and the transport layer for traffic switching).

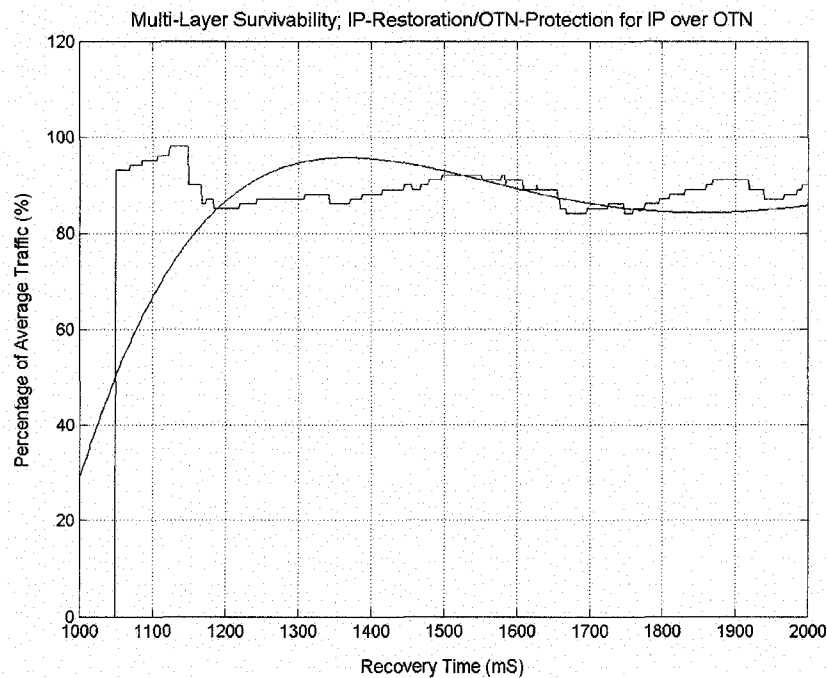


Fig. 4.19: Combined Multi-layer Survivability; IP Restoration/OTN Protection (post recovery view)

4.4.10. Combined Multi-layer Survivability; IP Restoration/SONET Protection

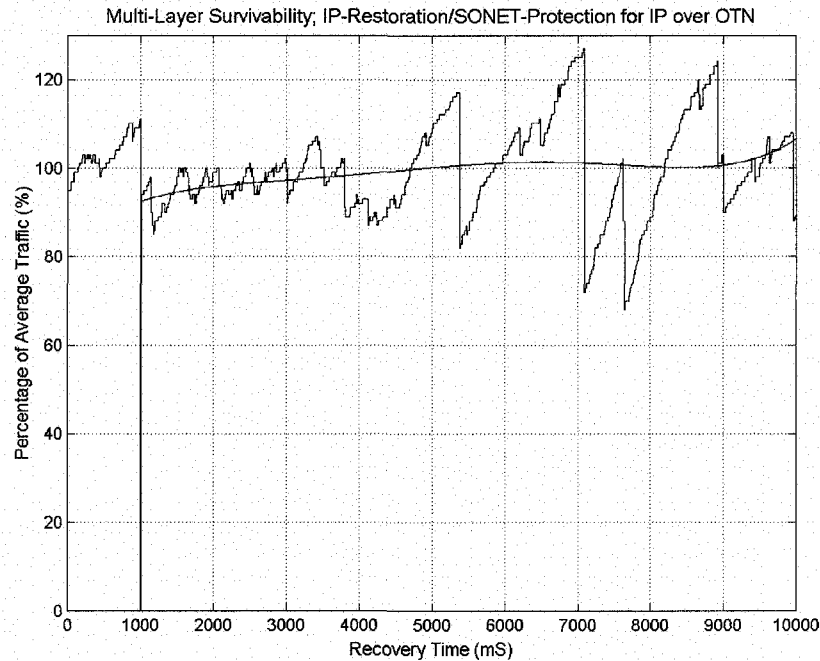


Fig. 4.20: Combined Multi-layer Survivability; IP Restoration/SONET Protection

The IP restoration/SONET protection combined multi-layer restoration simulation performance is shown in Fig. 4.20 and Fig. 4.21 with the following remarks:

- The IP is the only client in the network under discussion;
- The predicted survivability schemes demonstrates an enhancement in the outcome performance;
- Approximately 93% of the total affected traffic is restored immediately after the recovery process starts;
- Fault detection and processing take approximately 20ms, which can be considered as the total repair time (this is different from IP/OTN scheme),

- The 1+1 line protection concept is deployed in the simulation, and provides zero time switching between the working and protecting paths (we neglect the processing time taken from the management control plane and the transport layer for traffic switching).

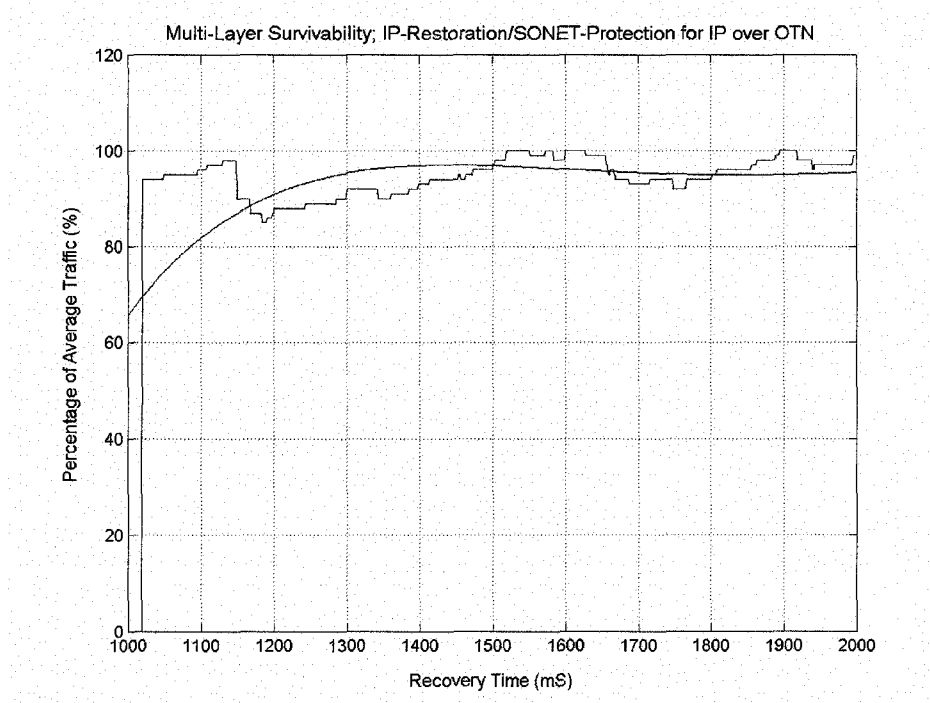


Fig. 4.21: Combined Multi-layer Survivability; IP Restoration/SONET Protection (post recovery view)

4.4.11. Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/OTN-Protection

The IP-MPLS protection and restoration/OTN protection combined multi-layer restoration simulation performance is shown in Fig. 4.22 and Fig. 4.23 with the following remarks:

- The IP is the only client in the network under discussion;
- The predicted survivability scheme demonstrates an optimum enhancement in the outcome performance;

- Approximately 93% of the total affected traffic is restored at the beginning of the recovery process starting;
- Fault detection and processing take approximately 20ms, which is part of the repair time,
- The 1+1 line protection concept is deployed in the simulation and provides zero time switching between the working and protecting paths (we neglect the processing time taken from the management control plane and the transport layer for traffic switching).

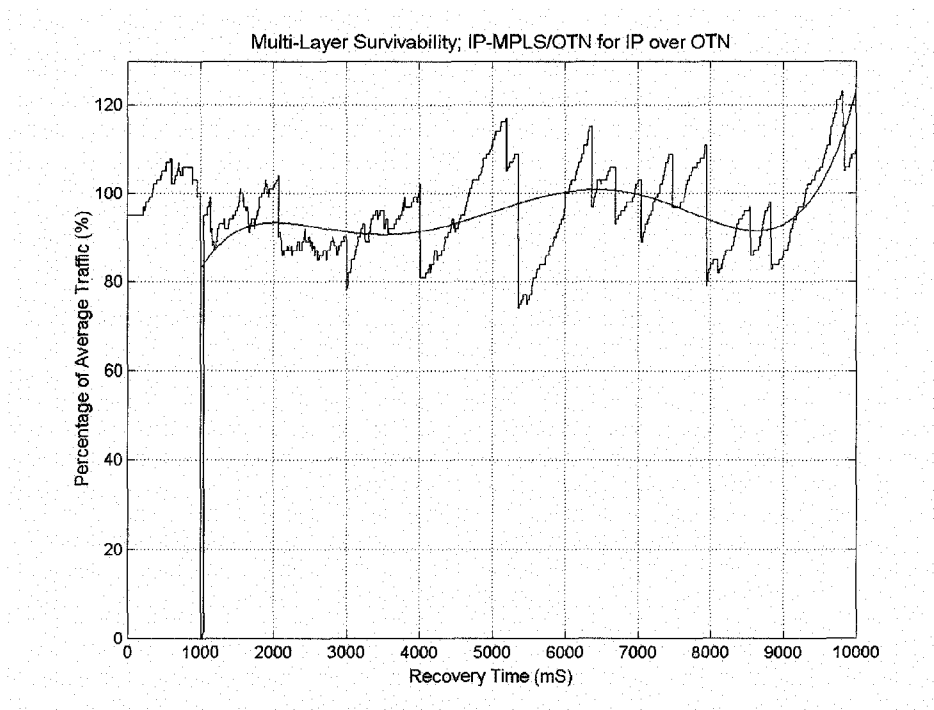


Fig. 4.22: Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/SONET-Protection

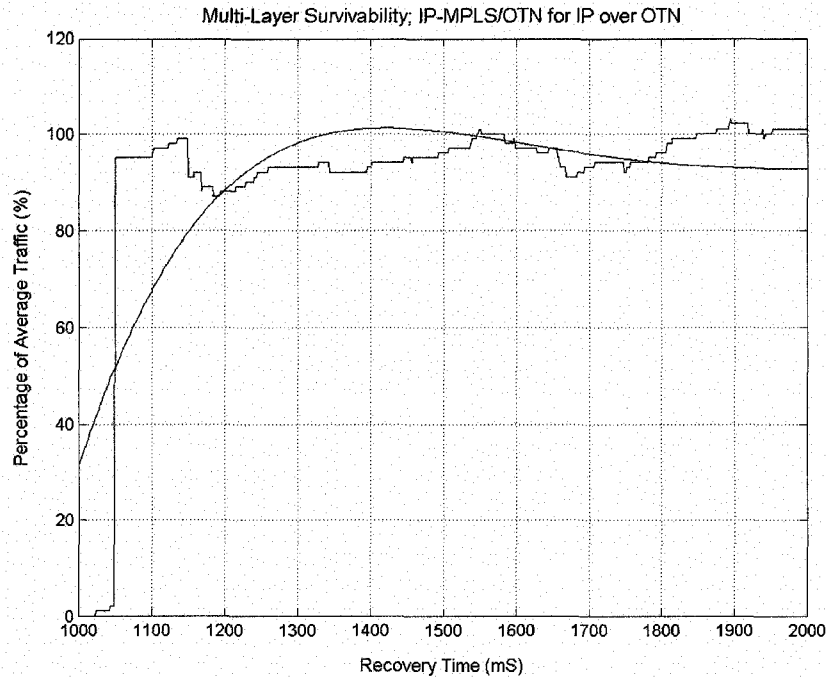


Fig. 4.23: Combined Multi-layer Survivability; IP-MPLS Protection and Restoration/SONET-Protection (post recovery view)

4.4.12. Simulation Graphs Comparison

The simulated network architectures for single-layer, multi-layer, and combined multi-layer schemes are grouped for comparison in Fig. 4.24, Fig. 4.25, and Fig. 4.26. Fig. 4.24 presents the simulation performances of the multi-layer survivability schemes when using only single-layer survivability functions. Fig. 4.25 presents the simulation performances of the multi-layer survivability schemes when deploying different multi-layer survivability strategies. Fig. 4.26 presents the simulation performances of the predicted multi-layer survivability schemes when deploying the integration concept of multi-layer survivability strategies. A tremendous improvement can be achieved to the network survivability if these concepts are deployed in existing networks.

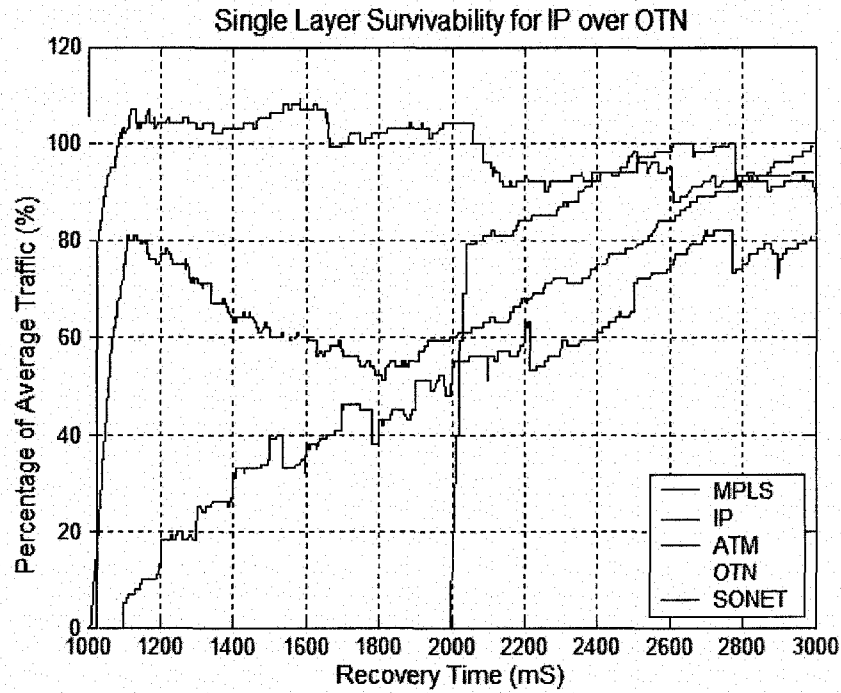


Fig. 4.24: Single layer Survivability (after recovery view)

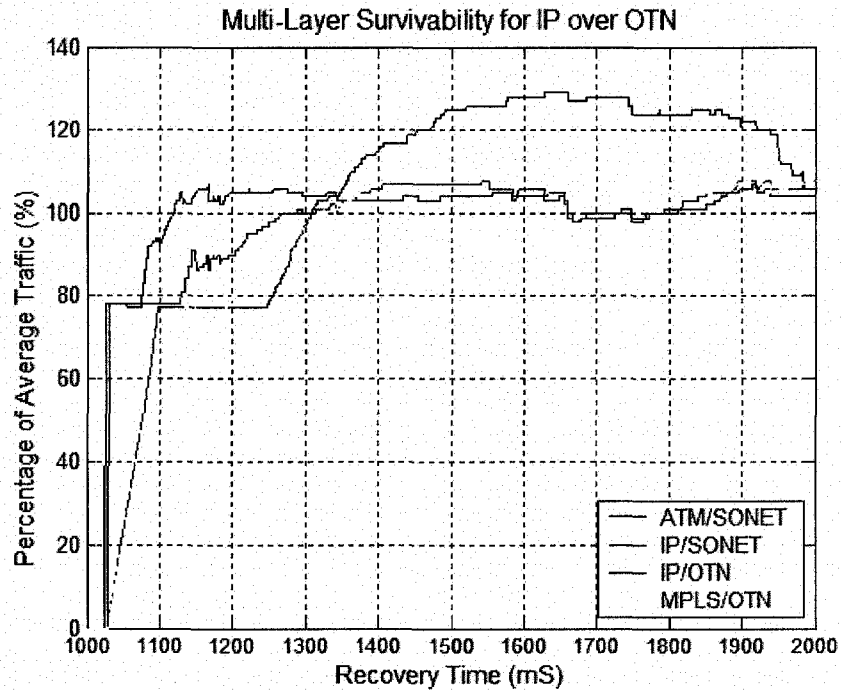


Fig. 4.25: Multi-layer Survivability (after recovery view)

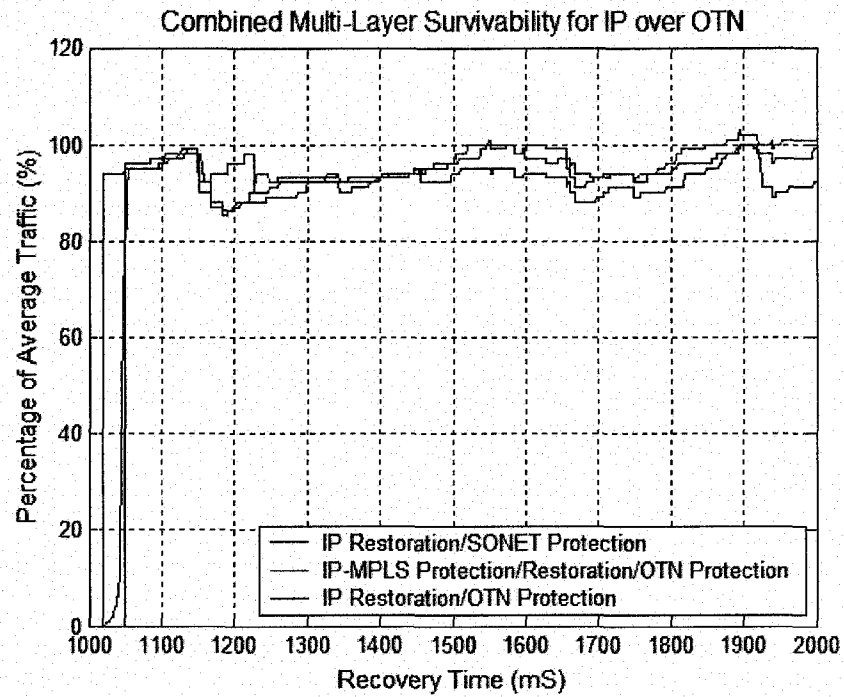


Fig. 4.26: Combined Multi-layer Survivability (after recovery view)

Chapter 5: Conclusions

Selecting a survivability strategy that fulfills all the requirements needed by a differentiated QoS in compromising between the overall network design and operation costs is not an easy task, especially in a multi-layer network environment.

We investigated through analysis and simulation different schemes for four network architectures: IP/ATM/SONET/OTN, IP/POS/OTN, IP/GbE/OTN and IP-MPLS/OTN. In the following sections we will summarize the outcomes of both the analysis and simulation for the network architectures used according to the survivability scheme implemented.

5.1. Single-Layer Restoration Schemes

Survivability functions available in the different network layers differ mainly in terms of; protection time, granularity, fault coverage and cost.

Assigning either restoration or protection to a lower layer leads all kinds of traffic to be treated at the same time with the same way. An operational cost reduction may be a result of that. On the other hand, assigning either restoration or protection to a higher layer enables QoP for different traffic QoS. Furthermore, we get moderately high level of survivability for the reason that the lower layers also survived from many types of failures.

The survivability functions in both SONET and OTN have a high degree of similarities; the switching time is almost the same, e.g., it is less than 50 ms automatic protection time in each of them. The things which makes SONET differs from OTN are its finer granularity, bigger total transport capacity, and interchangeable time-slots ADM's and XC's to avoid blocking. Wavelength conversion in OTN may be equivalent to interchangeable time-slots as time-slots in SONET, but its implementation cost is much higher.

ATM survivability functions are relatively different than SONET or OTN; its faults detection criteria is faster while its restoration time is longer than both of them.

The IP/ATM/SONET/OTN architecture is an evolution of an ATM/SONET backbone where IP is the major client protocol and OTN is brought in for bandwidth capacity increase and cost reduction. In this architecture, SONET protection is well developed, so it is better to continue using it than migrating to OTN, where IP is a robust restoration solution.

In the IP/SONET (POS)/OTN architecture, SONET provides only 1+1 Linear MSP (Multiplex Section Protection), whereas the OTN layer can provide fast protection at both OMS and OCh sub-layers. That is why OTN OCh is chosen to provide protection as the IP for restoration as survivability functions.

Lack of survivability functions at the GbE layer does not cause any weakness for the IP/GbE/OTN architecture as the OTN OCh protection as well as IP restoration can provide functions for the two survivability types.

In the IP-MPLS/OTN, MPLS supports finer and more flexible bandwidth granularity than re-configurable OTN and also differentiates the services between

traffic types. Therefore, one can choose to protect only these LSPs that have stringent QoS requirements. On the other hand, this finer granularity has a cost. To illustrate this, let us consider a case when a fiber goes out of service. The OTN protection needs to switch only a few wavelengths, while MPLS may deal with hundreds of LSPs. This reflects the traditional wisdom that protection on the higher layers is slower than on lower layers. So, using the lower OTN layer for service protection or restoration may simplify planning and guarantee faster recovery from a larger variety of failure scenarios. Also using MPLS for restoration may minimize spare capacity resources and costs.

Table 5.1 lists the selected Single Layer Survivability for the four analyzed Network architectures.

Table 5.1: Selected Single Layer Survivability for the Four Network Architectures

Architecture	Protection	Restoration
IP/ATM/SONET/OTN	SONET Path(OCh)	IP
IP/POS/OTN	OTN OCh	IP
IP/GbE/OTN	OTN OCh	IP
IP-MPLS/OTN	OTN OCh	MPLS

5.2. Multi-Layer Restoration Schemes

The seven survivability strategies examined in section 3.1 provide solutions for the multilayer architectures survivability. The problem exists in their survivability function duplications. While the concept of hold-off time is standardized in SONET networks, it is also proposed to the other services like ATM and OTN.

Coordination of inter-layer survivability actions through signaling between layers is also a good solution. It is realized by deploying the MPLS concept. MP λ S/GMPLS is the extension of the MPLS principle for the optical layer.

In IP/ATM/SONET/OTN architecture, the hold-off timer strategy is considered for the period time frame between the restorations functions of the SONET layer and the IP layer as well as the IP/SONET (POS)/OTN architecture. While in IP/GbE/OTN and IP-MPLS/OTN, the hold-off timer is considered for the period time frame between the restorations functions of the OTN layer and the IP layer.

Table 5.2 lists the selected Multi-layer Survivability schemes for the four Network architectures.

Table 5.2: Selected Multi-layer Survivability Schemes for the four Network Architectures

Architecture	Survivability Scheme
IP/ATM/SONET/OTN	SONET/IP - Restoration Hold-off time
IP/POS/OTN	SONET/IP - Restoration Hold-off time
IP/GbE/OTN	OTN/IP - Restoration Hold-off time
IP-MPLS/OTN	OTN/IP-MPLS - Restoration Hold-off time

5.3. Combined Survivability Schemes

Combining the traditional wisdom that protection on the higher layers is slower than on lower layers with the fact that the restoration at a higher layer is more robust and enables QoP for different QoS traffics seems to be an optimal survivability solution for multi-layer network architectures. The comprehensive analysis of the different architectures illustrated that the integration of the protection functions in the OTN or SONET layer (e.g. OCh protection) with the IP restoration functions is a good

strategy for multi-layer survivability. This is because it combines the benefits of the fast protection due to physical layer failures with wide fault coverage robust restoration. We therefore believe that we can meet the survivability requirements of both real-time and non-real-time traffic in the IP over OTN networks by introducing this combined solution.

The use of OTN protection with SONET protection is not suggested, because it may cause unwanted interaction between the layers, so in the IP/ATM/SONET/OTN architecture it is realistic to combine the SONET OCh protection with the IP restoration.

In IP/SONET (POS)/OTN and IP/GbE/OTN architectures, the OTN OCh protection offers fast recovery for an Optical layer single failure including transponders, while IP re-routing recovers other types of failures like router port failures or multiple failures. The substantial speed difference between these two survivability mechanisms avoids any unwanted interaction. The proposed combined solution for these architectures is realized by OTN OCh protection and IP restoration.

In the IP-MPLS/OTN architecture, MPLS supports finer and more flexible bandwidth granularity than re-configurable OTN and also differentiates the services between traffic types whereas we can choose to protect those LSPs only that have stringent QoS requirements. In addition to this, using the lower OTN layer for service protection, we can simplify planning and guarantee faster recovery from a larger variety of failure scenarios. Furthermore, we can choose to protect some of the wavelengths in the OTN layer (per wavelength) and protect the paths carried on the remaining wavelengths at a finer level by MPLS. The final decision is a matter of

trade-offs. These can be realized if we combine OTN OCh protection with IP-MPLS protection and restoration.

Table 5.3 lists the proposed Multi-layer Combined Survivability schemes for the four Network architectures.

Table 5.3: Proposed Multi-layer Combined Survivability Schemes for the Four Network Architectures

Architecture	Survivability Scheme
IP/ATM/SONET/OTN	SONET Path(OCh) protection / IP restoration
IP/POS/OTN	OTN OCh protection / IP restoration
IP/GbE/OTN	OTN OCh protection / IP restoration
IP-MPLS/OTN	OTN OCh protection / IP-MPLS protection and restoration

5.4. Future Research

A similar analysis needs to be done in the cases of (1) multiple failures, (2) wavelength (OTN) and/or time-slot (SONET) blocking, (3) network traffic engineering schemes other than load balancing, (4) other measures than the time elapsed from the occurrence of a failure to the return to average traffic levels, (5) other network architectures, (6) other multi-layer survivability strategies, (7) client protocols/traffic other than IP, (8) considering self-similarity traffic instead of Poisson model.

References

- [ALB06] S. Albarrak and D. Harle, "Pre-Allocated Restoration Technique in a Distributed GMPLS-Based IP/WDM Mesh Network", Proceedings IEEE Information and Communication Technologies ICTTA '06.2nd, Damascus, Syria, Vol. 2, April 2006, pp. 2236 – 2241.
- [ALL98] C. Allen, "Optical Link Quality Monitoring for OA&M- A White Paper", Lightwave Telecommunication Systems Laboratory, Information and Telecommunications Technology Center, University of Kansas, 1998.
- [AND94A] J. Anderson et al., "Fast Restoration of ATM networks", IEEE Journal on Selected Areas in Communications, Vol. 12, Issue 1, Jan. 1994, pp. 128 – 138.
- [AND97B] J. Anderson, C. Newton and T. Noh, "Virtual Path Group Protection Switching- A Method for Fast ATM Network Survivability", Bell Labs Technical Journal, Vol. 2, Issue 2, spring 1997, pp. 213 - 233.
- [ANSI01] ANSI T1.105-2001, "Synchronous Optical Network (SONET) - Basic Description including Multiplex Structure, Rates, and Formats", 2001.
- [ARA02] S. Arakawa and M. Murata, "Lightpath management of logical topology with incremental traffic changes for reliable IP over WDM networks", Optical Network Magazine, Vol. 3, May 2002, pp. 68 - 76.
- [ARA03] S. Arakawa and M. Murata, "Reliability Issues in IP over Photonic Networks", Chapter 2 of "Reliability, Survivability and Quality of Large Scale Telecommunication Systems" by Professor Peter Stavroulakis, ISBN: 9780470847701 John Wiley & Sons, 2003.

[ASL05] F. Aslam et al., "A Facility Based Computation Framework for Restoration Routing Using Aggregate Link Usage Information", Proceedings Quality of Service in Multiservice IP Networks Conference QoS-IP, Catania, Italy, Vol. 3375 of the series Lecture Notes in Computer Science by Springer-Verlag, Feb. 2005, pp. 150 - 163.

[ASL06] F. Aslam et al., "Bandwidth Sharing with Primary Paths for Restoration Routing in an MPLS Network", Proceedings 9th IEEE Global Internet Symposium 2006 in conjunction with IEEE INFOCOM 2006, Barcelona, Spain, April 2006, pp. 1 - 6.

[AUT98] A. Autenrieth et al., "Simulation and Evaluation of Multi-layer Broadband Networks", Proceedings First International Workshop on the Design of Reliable Communication Networks DRCN'98, Bruges, Belgium, May 1998, pp. 40.

[AYB01] G. Aybay et al., "An Introduction to Resilient Packet Ring Technology", White Paper, Resilient Packet Ring Alliance, October 2001.

[BELL93] Bellcore, "Digital Cross-Connect Systems in Transport Network Survivability", Bellcore Special Report, Issue 1, January 1993

[BELL96] Bellcore, "ATM Virtual Path Functionality in SONET Rings -Generic Criteria", Bellcore Standard GR-2837-CORE, Issue 3, Oct. 1996.

[BIS96] M. Bischoff, M. Huber and O. Jahreis, "Operation and Maintenance for an All-Optical Transport Network", IEEE Communications Magazine, Vol. 34, Issue 11, Nov. 1996, pp. 136 – 142.

[BLA00] U. Black, "IP Routing Protocols; RIP, OSPF, BGP, PNNI & Cisco Routing Protocols", ISBN-13: 978-0-13-014248-1, Upper Saddle River, NJ Prentice Hall, Feb. 2000.

[BON01] P. Bonenfant and A. Rodriguez, "Framing Techniques for IP over Fiber", IEEE Network Magazine, Vol. 15, Issue 4, July-Aug. 2001, pp. 12 – 18.

[BON98] M. Bonnifait, H. Ohta, and J. Manchester, "ITU-T ongoing studies on ATM protection switching", Proceedings First International Workshop on the Design of Reliable Communication Networks DRCN'98, Bruges, Belgium, May 1998, pp. 12.

- [BRA92] T. Bradley, C. Brown and A. Malis, "Multiprotocol Interconnect over Frame Relay", RFC1294, IETF Network Working Group, January 1992.
- [CAR00] J. Carlson, "PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing", RFC 2823, IETF Network Working Group, May 2000.
- [CHA94] C. Chao, G. Fuoco, and D. Kropfl, "Faster Platform Gives the Network A Competitive Edge", AT&T Technology Journal, July/August 1994, pp. 69–81.
- [CHE96] S. Chen et al., "An Efficient Spare Capacity Allocation Strategy for ATM Survivable Networks", Proceedings IEEE Global Telecommunications Conference GLOBECOM '96, London, UK, Vol. 1, Nov. 1996, pp. 442 – 446.
- [CHI04] C. Chigan, G. Atkinson and R. Nagarajan, "Simplified Mathematical Modeling of Joint Multilayer Network Restoration via Sampling Technique", Applied Telecommunications Symposium, Arlington, Virginia, 2004, The Society for Modeling & Simulation International (SCS) document ID: 1633.
- [CIS06] Cisco Networks, "Using HSRP for Fault-Tolerant IP Routing", White Paper, August 2006.
- [COR01] Corrigent Systems, Inc., "Resilient Packet Ring Technology Overview", Technical Note, 2001.
- [DEA94] A. Deacon, "Network Reliability Better Than Ever," AT&T Technology, Journal 1994, Vol. 7, Issue 4, pp. 20–23.
- [DEM97] P. Demeester, M. Gryseels and K. Struyve, "PANEL - Protection Across Network Layers", Proceedings of the European Conference on Networks and Optical Communications NOC '97, Antwerp, Belgium, 1997, pp. 303 - 311.
- [DEM99] P. Demeester et al., "Resilience in Multilayer Networks", IEEE Communications Magazine, Vol. 37, Issue 8, Aug. 1999, pp. 70 - 76.
- [ELL99] R. Ellison et al., "Survivable Network Systems: An Emerging Discipline", Survivable Network Technology Team CERT® Technical Report, November 1997, Revised May 1999.

- [FUJ96] N. Fujii, I. Yoda, and K. Minato, "An ATM Transport Network Operation System Based on TMN", Proceedings IEEE/IFIP Network Operations and Management Symposium, 1996, Vol. 1, April 1996, pp. 124 - 134.
- [FUM00] A. Fumagalli, L. Valcarenghi, "IP restoration vs. WDM protection: is there an optimal choice?", IEEE Network Magazine, Vol. 14, Issue 6, Nov.-Dec. 2000, pp. 34 - 41.
- [GER97] O. Gerstel, R. Ramaswami and G. Sasaki, "Fault-tolerant multi-wavelength optical networks with limited wavelength conversion", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue 7, Sept. 1998, pp. 1166 - 1178.
- [GHA03] N. Ghani, S. Dixit and T. Wang, "On IP-WDM integration: a retrospective", IEEE Communications Magazine, Vol. 41, Issue 9, Sept. 2003, pp. 42 - 45.
- [GHA06] N. Ghani et al., "Multi-Tiered Services in Next-Generation SONET/SDH Networks", Proceedings IEEE International Conference on Communications ICC '06, Istanbul, Turkey, Vol. 6, June 2006, pp. 2495 - 2500.
- [GOR05] S. Gorshe, "SONET/SDH Technology White Paper", PMC-2030895 (3.0), PMC-Sierra, Inc., March 2005.
- [GRO87] W. Grover, "The self-healing network", Proceedings IEEE Global Telecommunications Conference GLOBECOM '87, Tokyo, Japan, Nov. 1987, pp. 1090 - 1095.
- [GRY98A] M. Gryseels and P. Demeester, "Survivability design in multi-layer transport networks", Proceedings of the 6th International Conference on Telecommunication Systems, Nashville, TN, March 1998, pp. 302 - 312.
- [GRY98B] M. Gryseels, R. Clemente, and P. Demeester, "Common pool survivability in ATM over SDH ring networks", Proceedings International Workshop in the Design of Reliable Communication Networks DRCN '98, Bruges, Belgium May 1998.
- [GRY98C] M. Gryseels et al., "A Cost Evaluation of Service Protection Strategies in ATM on SDH Transport Networks", Proceedings of the 1st International Workshop

on the Design of Reliable Communication Networks DRCN '98, Bruges, Belgium, May 1998, pp. 38.

[HED88] C. Hedrick, "Routing Information Protocol", RFC1058, IETF Network Working Group, June 1988.

[HEI93] J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 1483, IETF Network Working Group, July 1993.

[HEI99] J. Heinanen et al., "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, IETF Network Working Group, September 1999.

[HER96] M. Herzberg and A. Utano, "Optimal Assignment of Spare Capacity to Back-up VPs in Survivable ATM Networks", Proceedings Networks '96, Sydney, Australia, 1996, pp. 665–670.

[HO02A] P. Ho and H. Mouftah, "A framework of scalable optical metropolitan networks for improving survivability and class of service", IEEE Network Magazine, Vol. 16, Issue 4, July-Aug. 2002, pp. 29 – 35.

[HO02B] P. Ho and H. Mouftah, "A framework for service-guaranteed shared protection in WDM mesh networks", IEEE Communications Magazine, Vol. 40, Issue 2, Feb. 2002, PP. 97 – 103.

[HO04A] P. Ho and H. Mouftah, "Shared protection in mesh WDM networks", IEEE Communications Magazine, Vol. 42, Issue 1, Jan 2004, pp. 70 – 76.

[HO04B] P. Ho, J. Tapolcai and H. Mouftah, "On achieving optimal survivable routing for shared protection in survivable next-generation Internet", IEEE Transactions on Reliability, Vol. 53, Issue 2, June 2004, pp. 216 – 225.

[HO04C] P. Ho and H. Mouftah, "Reconfiguration of spare capacity for MPLS-based recovery in the Internet backbone networks", IEEE/ACM Transactions on Networking, Vol. 12, Issue 1, Feb. 2004, pp. 73 – 84.

[HO06] K. Ho and K. Cheung, "A New Planning Methodology for IP Networks with Dynamic Traffic Demand and Full Survivability Guarantee against Link Failures",

Proceedings International Conference on Internet Surveillance and Protection ICISP '06, Cap Esterel, Côte d'Azur, France, August 2006, pp. 22.

[HOU96] C. Hou, "Design of a Fast Restoration Mechanism for Virtual Path- Based ATM Networks", Proceedings IEEE INFOCOM '97 and Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 1, April 1997, pp. 361 - 369.

[HUO06] W. Huo, C. Assi and A. Shami, "Multiple-Link Failures Survivability in Optical Networks with Traffic Grooming Capability", Proceedings IEEE International Conference on Communications ICC '06, Istanbul, Turkey, Vol. 6, June 2006, pp. 2811 – 2816.

[HWA01] L. Hwajung, C. Hongsik and C. Hyeong, "Restoration in IP over WDM optical networks", Proceedings International Conference on Parallel Processing Workshops ICCP '01, Valencia, Spain, Sept. 2001, pp. 263 – 268.

[IMA06] W. Imajuku et al., "Design of MPLS/GMPLS multilayer network considering protection and restoration", Proceedings Optical Fiber Communication Conference OFC '06 and the 2006 National Fiber Optic Engineers Conference NFOEC '06, Anaheim , California, March 2006, pp. 3.

[INT00] Intel Corporation, "Gigabit Ethernet Over Copper", White Paper, April 2000.

[INT05] Intel and Cisco, "Gigabit Ethernet Over Fiber and Copper" White Paper, Gigabit and 10 Gigabit Ethernet Solutions, June 2005.

[INT06] Intel Corporation, "10 Gigabit Ethernet Expands Network Bandwidth and Shrinks Latency", White Paper, February 2006.

[ITU00A] ITU-T G.707, "Network node interface for the synchronous digital hierarchy (SDH)", October 2000.

[ITU00B] ITU-T Recommendation G.805, "Generic Functional Architecture of Transport Networks", March 2000.

[ITU01A] ITU-T G.7041, "Generic Framing Procedures", December 2001.

- [ITU01B] ITU-T G.7042, "Link capacity adjustment scheme (LCAS) for virtual concatenated signals", November 2001.
- [ITU01C] ITU-T G.872, "Architecture of Optical Transport Networks", November 2001.
- [ITU02] ITU-T G.798, "Characteristics of optical transport network hierarchy equipment functional blocks", January 2002.
- [ITU03A] ITU-T G.709, "Interfaces for the Optical Transport Network", March 2003.
- [ITU03B] ITU-T G.873.1, "Optical Transport Network (OTN): Linear Protection", March 2003.
- [ITU92] ITU-T Draft Recommendation, "(I.ps): B-ISDN operation and maintenance principles and functions", 1992.
- [ITU95] ITU-T Recommendation G.841, "Types and Characteristics of SDH Network Protection Architectures", July 1995.
- [ITU96] ITU-T Recommendation G.783, "Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks," 1996.
- [ITU96] ITU-T Recommendation I.363.5, "B-ISDN ATM Adaptation Layer specification: Type 5 AAL", August 1996.
- [ITU97A] ITU-T Draft Recommendation, "(I.ps): ATM Network Survivability Architecture and Mechanisms", 1997.
- [ITU97B] ITU-T Draft Recommendation, "(I.ps): ATM Network Survivability Architecture and Mechanisms", 1997.
- [ITU98] ITU-T Recommendation G.841, "Types and characteristics of SONET network protection architectures", October 1998.
- [JIA02] K. Jia, L. Mason and Q. Yang, "Two-layer restoration scheme for IP over optical networks with MPLS", Proceedings the 8th IEEE International Conference on Communication Systems ICCS '02, Singapore, Vol. 2, Nov. 2002, pp. 923 – 927.

- [JOH96] D. Johnson, "Survivability strategies for broadband networks", Proceedings IEEE Global Telecommunications Conference GLOBECOM '96, London, UK, Vol. 1, Nov. 1996, pp. 452 – 456.
- [KAJ94] Y. Kajiyama, N. Tokura, and K. Kikuchi, "An ATM VP-Based Self-Healing Ring", IEEE Journal on Selected Areas in Communications, Vol. 12, Issue 1, Jan. 1994, pp. 171–178.
- [KAW94] R. Kawamura, K. Sato and I. Tokizawa, "Self-Healing ATM Networks Based on Virtual Path Concept", IEEE Journal on Selected Areas in Communications, Vol. 12, Issue 1, Jan. 1994, pp. 120 – 127.
- [KAW95A] R. Kawamura and I. Tokizawa, "Self-healing Virtual Path Architecture in ATM Networks", IEEE Communications Magazine, Vol. 33, Issue 9, Sept. 1995, pp. 72–79.
- [KAW95B] R. Kawamura, H. Hadama, and I. Tokizawa, "Implementation of Self healing Function in ATM Networks based on Virtual Path Concept", Proceedings IEEE INFOCOM '95, Boston, MA, Vol. 1, April 1995, pp. 303 – 311.
- [KAW96] R. Kawamura and S. Ohta. "Self-healing ATM network architecture; Implementation results from NTT's nationwide testbed ATM network", Proceedings Networks '96, Sydney, Australia, 1996, pp. 717–722.
- [KAW98A] R. Kawamura, T. Yahara, and H. Uematsu, "Self-healing ATM Network Architecture and Their Field Deployment", Proceedings International Workshop in the Design of Reliable Communication Networks DRCN '98, Bruges, Belgium, May 1998.
- [KAW98B] R. Kawamura, "A Failure-Resistant Self-healing Scheme in ATM Networks", IEICE Transactions on Communications, Vol. E81-B, Issue 4, 1998.
- [KAW98C] R. Kawamura, "Architectures for ATM Network Survivability", IEEE Communications Surveys, Fourth Quarter 1998, Vol. 1, Issue 1, Oct. 1998, pp. 2 – 10.
- [KAW99] R. Kawamura and H. Ohta, "Architectures for ATM network survivability and their field deployment", IEEE Communications Magazine, Vol. 37, Issue 8, Aug. 1999, pp. 88 – 94.

- [KOD01] M. Kodialam and T. Lakshman, "Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information", *Proceedings IEEE INFOCOM 2001*, Vol. 1, April 2001, pp. 376 – 385.
- [KOH96] J. Koh et al., "A Genetic Algorithm for Backup Virtual Path Routing in Restoration of ATM Networks", *Proceedings Networks '96*, Sydney, Australia, 1996, pp. 639–644.
- [LAB99] C. Labovitz, A. Ahuja, and F. Jahanian, "Experimental Study of Internet Stability and Wide-Area Backbone Failures", *Proceedings of the Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing*, June 1999.
- [LAK02] S. Lakshmanan et al., "An IP-centric control plane for survivable WDM mesh networks: experimental results on the OMEGA test-bed ", *IEEE Workshop on IP Operations and Management IPOM '02*, Dallas, Texas, Oct. 2002, pp. 154 – 158.
- [LEE01A] H. Lee, H. Choi, and H. Choi, "IP Restoration on WDM Optical Networks", *Proceedings 35th Conference of Information Science and Systems CISS '01*, Baltimore, Maryland, Vol. 1, March 2001, pp. 268.
- [LEE01B] H. Lee, H. Choi, and H. Choi, "Restoration in IP over WDM Optical Networks", *IEEE International Conference on Parallel Processing Workshops ICPP '01*, Valencia, Spain, Sept. 2001, pp. 263 - 268.
- [LEE01C] H. Lee et al., "Survival Logical Topology Design in WDM Optical Ring Networks", *Proceedings 39th Allerton conference on communications, control, and computing*, University of Illinois at Urbana-Champaign, Oct. 2001.
- [LEE02A] H. Lee, H. Choi, and H. Choi, "Reconfiguration of Survivable Logical Topologies in WDM Ring Networks", *Proceedings 36th Conference of Information Science and Systems CISS '02*, Princeton University, March 2002.
- [LEE02B] H. Lee et al., "Preserving Survivability During Logical Topology Reconfiguration in WDM Ring Networks", *Proceedings IEEE International Conference on Parallel Processing Workshops ICPP '02*, Vancouver, BC, Canada, Aug. 2002, pp. 224 - 230.

- [LEE03] H. Lee et al., "Survival Embedding of Logical Topology in WDM Ring Networks", *International Journal of Information Science*, Vol. 149, Issues 1-3, Jan. 2003, pp. 151-160.
- [LI06] Li Li et al., "Routing bandwidth guaranteed paths with local restoration in label switched networks", *IEEE Journal on Selected Areas in Communications*, Vol. 23, Issue 2, Feb 2005, pp. 437 – 449.
- [LIE94] S. Liew and K. Lu, "A Framework for Characterizing Disaster-Based Network Survivability", *IEEE Journal on Selected Areas in Communications*, Vol. 12, Issue 1, Jan. 1994, pp. 52 – 58.
- [LIN04] L. Lindholm and L. Petersen, "Scalable Router-based Network Node", *United States Patent 20040260834*, December 2004.
- [LIN94] N. Lin, A. Zolfaghari and B. Lusignan, "ATM Virtual Path Self-Healing Based on a New Path Restoration Protocol", *Proceedings IEEE GLOBECOM '94*, Vol. 2, Dec. 1994, pp. 794 – 798.
- [LON01] K. Long et al., "A New Approach to Multi-layer Network Survivability: Strategies, Model and Algorithm", *Journal of High Speed Networks JHSN*, special issues on "Survivable Optical Networks", Vol.10, Issue 2, Sep. 2001, pp. 127-134.
- [MAI02] G. Maier, A. Pattavina and S. De Patre, "Optical Network Survivability: Protection Techniques in the WDM Layer", *Photonic Network Communications*, Vol. 4, Issues 3-4, July 2002, pp. 251-269.
- [MAL99] A. Malis, "PPP over SONET/SDH", *RFC 2615, IEFT Network Working Group*, June 1999.
- [MED95] D. Medhi and R. Khurana, "Optimization and Performance of Network Restoration Schemes for Wide-Area Teletraffic Networks", *Journal of Network and Systems Management*, Vol. 3, No. 3, September 1995, pp. 265 - 294.
- [MEL06] D. Mello et al., "Specification of SLA Survivability Requirements for Optical Path Protected Connections", *Proceedings Optical Fiber Communication Conference OFC '06 and the 2006 National Fiber Optic Engineers Conference*, Anaheim California, March 2006, pp. 3.

- [MOU02] H. Mouftah and P. Ho, "Optical Networks: Architecture and Survivability", Springer Publisher, ISBN 978-1-4020-7196-6, December 2002.
- [MUR00] M. Murata, "Reliability issues in IP over WDM networks", Proceedings IEEE International Workshop on Telecommunications, April 2000.
- [MUR97] K. Murakami and H. Kim, "Comparative Study on Restoration Schemes of Survivable ATM Networks", Proceedings IEEE INFOCOM '97 and Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Kobe, Japan, Vol. 1, April 1997, pp. 345 – 352.
- [NAG96] N. Nagatsu, S. Okamoto and K. Sato, "Large Scale Photonic Transport Network Design Based on Optical Paths", Proceedings IEEE Global Telecommunications Conference GLOBECOM '96, London, UK, Vol. 1, Nov. 1996, pp. 321 – 327.
- [NAG97] A. Nagarajan and V. Frost, "Service Survivability of Fiber Networks: Photonic Networks, SONET and ATM - A Technical Report", Information and Telecommunication Technology Center, University of Kansas, ITTC-FY97-TR-12120-2, April 1997.
- [NAS04A] H. Naser and H. Mouftah, "A multilayer differentiated protection services architecture", IEEE Journal on Selected Areas in Communications, Vol. 22, Issue 8, Oct. 2004, PP. 1539 – 1547.
- [NAS04B] H. Naser and H. Mouftah, "Availability analysis and simulation of mesh restoration networks", Proceedings Ninth IEEE International Symposium on Computers and Communications ISCC '04, Alexandria, Egypt, Vol. 2, June- July 2004, pp. 779 – 785.
- [NAT03] National Communications System, "Internet Protocol over Optical Transport Networks", Technical Information Bulletin 03-3, December 2003.
- [NED95A] L. Nederlof et al., "End-to-end Survivable Broadband Networks", IEEE Communications Magazine, Vol. 33, Issue 9, Sept. 1995, pp. 63 – 70.
- [NED95B] L. Nederlof, H. Vanderstraeten, and L. Hauwermeiren, "Development, Evaluation and Implementation of a Distributed Restoration Algorithm", Proceedings

International Symposium on Internet and B-ISDN ISIB '95, Beijing, China, Apr. 1995.

[NEW96] P. Newman et al., "Transmission of Flow Labelled IPv4 on ATM Data Links Ipsilon Version 1.0", RFC 1954, IETF Network Working Group, May 1996.

[NIS95] K. Nishihata, "SDH-based 52Mb/s Digital Cross-connect Systems with hit-less function, TMN-based operation system", Proceedings IEEE DCS Workshop VI, Banff, Canada, June 1995.

[OHT96] S. Ohta and K. Nunokawa, "Comparison of Alternative Service Protection Mechanisms for Wide Area ATM Networks", Proceedings Networks '96, Sydney, Australia, 1996, pp. 281–286.

[OKI95] E. Oki, N. Yamanaka, and F. Picho, "Multiple-Availability-Level ATM Network Architecture", IEEE Communications Magazine, Vol. 33, Issue 9, Sept. 1995, pp. 80 – 88.

[OTS06] Y. Otsuga et al., "Implementation and Evaluation of a Multi-Layered Network Management system for GMPLS Networks", Proceedings 10th IEEE/IFIP Network Operations and Management Symposium NOMS '06, Vancouver, B.C., Canada, Apr. 2006, pp. 569 - 577.

[PIC06] M. Pickavet et al., "Recovery in Multilayer Optical Networks", IEEE Journal of Lightwave Technology, Vol. 24, Issue 1, Jan. 2006, pp.122 – 134.

[POS81] J. Postel, "Internet Control Message Protocol", RFC 792, IETF Network Working Group, September 1981.

[PRY91] M. de Prycker, "Asynchronous Transfer Mode: Solution for B-ISDN", Ellis Horwood, London, U K, 1991.

[QIN03] Y. Qin, L. Maso and K. Jia, "Study on a joint multiple layer restoration scheme for IP over WDM networks", IEEE Network Magazine, Vol. 17, Issue 2, March-April 2003, pp. 43 – 48.

- [RAM96] R. Ramaswami and K. Sivarajan, "Design of Logical Topologies for Wavelength-Routed Optical Networks", IEEE Journal on Selected Areas in Communications, Vol. 14, Issue 5, June 1996, pp. 840 – 851.
- [RAT06] K. Ratnam, L. Zhou and M. Gurusamy, "Efficient Multi-Layer Operational Strategies for Survivable IP-over-WDM Networks", IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 8, Part Supplement, Aug 2006, pp.16 - 31.
- [RAZ06] S. Raza et al., "Online routing of bandwidth guaranteed paths with local restoration using optimized aggregate usage information", IEEE International Conference on Communications ICC 2005, Istanbul , Turkey, Vol. 1, May 2005, pp. 201 – 207.
- [ROS01] E. Rosen, A. Viswanathan and R. Callon, "Multi-protocol Encapsulation over ATM Adaptation Layer 5", RFC 3031, IETF Network Working Group, Jan. 2001.
- [SAI94] H. Saito, "Teletraffic technologies in ATM networks", Artech House Inc., 1994.
- [SAS03] G. Sasaki and C. Su, "The Interface between IP and WDM and Its Effect on the Cost of Survivability", IEEE Communications Magazine, Vol. 41, Issue 1, Jan. 2003, pp. 74 – 79.
- [SAT96] K. Sato, "Advances in Transport Network Technologies: Photonic Networks, ATM, and SDH", Artech House Inc., 1996.
- [SCE95] L. Scerbo, "Readout of NRC Study on the Implementation and Maintenance of DCSs.", Proceedings IEEE DCS Workshop VI, Banff, Canada, June 1995.
- [SCH04] D. Schupke, "A Throughput Study of RPR Networks Subject to Single Failures", Munich University of Technology, 2004.
- [SHE06] Q. She, X. Huang, and P. Jason, "Maximum Survivability under Multiple Failures", Proceedings Optical Fiber Communication Conference OFC '06 and the 2006 National Fiber Optic Engineers Conference NFOEC '06, Anaheim , California, March 2006, pp. 3.

- [SIC06] A. Sichani, and H. Mouftah, "Performance Evaluation of Dynamic Restoration Techniques for Survivable Optical Networks", Proceedings 11th IEEE Symposium on Computers and Communications ISCC '06, Sardinia, Italy, June 2006, pp. 961 – 966.
- [SIM03] G. Simo, "Updates to key system acceptance tests for G.709 based long haul systems", White Paper, Nortel Networks, Photonics Systems Engineering, August 2003.
- [SIM93] W. Simpson, "PPP in HDLC Framing", RFC 1549, IEFT Network Working Group, December 1993.
- [SIM94A] W. Simpson, "PPP in HDLC-like Framing", RFC 1662, IEFT Network Working Group, July 1994.
- [SIM94B] W. Simpson, "PPP over SONET/SDH", RFC 1619, IEFT Network Working Group, May 1994.
- [SIM94C] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, IEFT Network Working Group, July 1994.
- [SON06] L. Song, J. Zhang, and B. Mukherjee, "The Advantages of Backup Reprovisioning After Failure Repair (and Failure Arrival) in Telecom Mesh Networks", IEEE International Conference on Communications ICC '06, Istanbul, Turkey, Vol. 6, June 2006, pp. 2501 – 2505.
- [SOS94] J. Sosnosky, "Service Applications for SONET DCS Distributed Restoration", IEEE Journal on Selected Areas in Communications, Vol. 12, Issue 1, Jan. 1994, pp. 59 – 68.
- [SOS95] J. Sosnosky and H. Kobrinski. "A Current Bellcore View of SONET ATM VP Rings", IEEE Global Telecommunications Conference GLOBECOM '95, Singapore, Vol. 1, Nov. 1995, pp. 39 – 44.
- [STA02] W. Stallings, "High-Speed Networks and Internets; Performance and Quality of Service", Upper Saddle River, NJ: Prentice Hall, 2002.

- [STA06] D. Staessens et al., "A Quantitative Comparison of Some Resilience Mechanisms in a Multidomain IP-over-Optical Network Environment", IEEE International Conference on Communications ICC '06, Istanbul, Turkey, Vol. 6, June 2006, pp. 2512 – 2517.
- [STR79] V. Strazisar, "Gateway Routing: An Implementation Specification", IEN 30, Bolt Beranek and Newman, April 1979.
- [STR96] K. Struyve and P. Demeester, "Escalation between Recovery: Beyond ATM Backup Recovery", Proceedings IEEE Global Telecommunications Conference GLOBECOM '96, London, UK, Communications, Vol. 1, Nov. 1996, pp. 755 – 761.
- [TAD96] Y. Tada, et al., "OA & M Framework for Multi-wavelength Photonic Transport Networks", IEEE Journal on Selected Areas in Communications, Vol. 14, Issue 5, June 1996, pp. 914-922.
- [TIA06] L. Tianjian and B. Wang, "On Optimal Survivability Design under a Scheduled Traffic Model in Wavelength-Routed Optical Mesh Networks", Proceedings of the 4th Annual Communication Networks and Services Research Conference CNSR'06, New Brunswick, Canada, May 2006, pp. 26 - 33.
- [TIA93] T1A1.2, Working Group on Network Survivability Performance, "A Technical Report on Network Survivability Performance", Report No. 24, November 1993.
- [VAJ06] K. Vajanapoom and D. Tipper, "Risk Reduction Based Survivable WDM Network Design", 25th IEEE International Performance, Computing, and Communications Conference IPCCC 2006, Phoenix, AZ, April 2006, pp. 8.
- [VEI96] P. Veitch, I. Hawker and G. Smith, "Administration of Restorable Virtual Path Mesh Networks", IEEE Communications Magazine, Vol. 34, Issue 12, Dec. 1996, pp. 96 – 101.
- [VEI97] P. Veitch and D. Johnson, "ATM Network Resilience", IEEE Network Magazine, Vol. 11, Issue 5, Sept.-Oct. 1997, pp. 26 – 33.
- [VOG01] M. Vogt, R. Martens and T. Andvaag, "Technical Report on a Reliability/Availability Framework for IP-based Networks and Services",

Proceedings Fourth International Workshop on Design of Reliable Communication Networks DRCN '03, Banff, Alberta, Canada, Oct. 2003, pp. 167 – 172.

[WAN05] H. Wang and H. Mouftah, “P-cycles in multi-failure network survivability”, Proceedings 7th International Conference on Transparent Optical Networks ICTON '05, Barcelona, Spain, Vol. 1, July 2005, pp. 381 – 384.

[WAU96] N. Wauters and P. Demeester, “Multiwavelength Cross-Connected Networks”, IEEE Journal on Selected Areas in Communications, Vol. 14, Issue 5, June 1996, pp. 881 – 892.

[WIL98] M. Wilson, “The Quantitative Impact of Survivable Network Architectures on Service Availability”, IEEE Communications Magazine, Vol. 36, Issue 5, May 1998, pp. 122 – 126.

[WU92] T. Wu, “Fiber Network Service Survivability,” Artech House, 1992.

[WU95] T. Wu, “Emerging Technologies for Fiber Network Survivability,” IEEE Communications Magazine, Vol. 33, Issue 2, Feb. 1995, pp.58 - 59, 62-74.

[XIO97] Y. Xiong and L. Mason, “Restoration Strategies and Spare Capacity Requirements in Self-healing ATM Networks”, IEEE/ACM Transactions on Networking, Vol. 7, Issue 1, Feb. 1999, pp. 98 – 110.

[YAH97] T. Yahara and R. Kawamura. “Virtual Path Self-healing Scheme based on Multi-Reliability ATM Network Concept,” IEEE Global Telecommunications Conference GLOBECOM '97, Phoenix, Arizona, Vol. 3, Nov. 1997, pp. 1803 - 1807.

[YAH98] T. Yahara, R. Kawamura and S. Ohta, “Multi-reliability Self-healing Scheme that Guarantees Minimum Cell Rate”, Proceedings International Workshop in the Design of Reliable Communication Networks DRCN' 98, Bruges, Belgium, May 1998.

[YIN00] Y. Yinghua, S. Dixit, and M. Ali, “On joint protection/restoration in IP-centric DWDM based optical transport networks”, IEEE Communications Magazine, Vol. 38, Issue 6, June 2000, pp. 174 – 183.

- [YIN01] Y. Yinghua et al., "A simple dynamic integrated provisioning/protection scheme in IP over WDM networks", IEEE Communications Magazine, Vol. 39, Issue 11, Nov. 2001, pp. 174 – 182.
- [YOS93] N. Yoshikai and T. Wu, "Message control channel protocol and performance analysis for distributed ATM Virtual Path self-healing network", IEEE Global Telecommunications Conference 1993 GLOBECOM '93, Houston, Texas, Vol. 3, Nov.- Dec. 1993, pp. 1589 - 1595.
- [ZHA02] H. Zhang, A. Durresi, "Differentiated multi-layer survivability in IP/WDM networks", Proceedings IEEE/IFIP Network Operations and Management Symposium NOMS '02 , Florence, Italy, April 2002, pp. 681 – 694.
- [ZHO00] D. Zhou and S. Subramaniam, "Survivability in Optical Networks", IEEE Network Magazine, Vol. 14, Issue 6, Nov.-Dec. 2000, pp.16 - 23.

Appendix A: Network Failures

In order to perform network survivability in a suitable way, we need to identify and classify the common physical failures. Some of them are listed below:

- Router failures; interface cards,
- In-site connections, e.g., those between router and optical equipment,
- OTN terminal equipment's optical amplifiers,
- OTN MUX/DEMUX,
- OTN equipment transponder cards,
- In-line optical amplifier,
- Fiber or cable cuts,
- whole equipment failure,
- Entire node failure,

Table A.1 lists the above failures with and some possible causes for them.

Table A.1: List of Failure Types and Possible Causes [LAB99]

Failure type	Possible causes
Router interface cards	Aging
In-site connections	Human error
OTN terminal equipment's optical amplifiers	Aging
OTN Mux/demux	Aging
Transponders	Aging
In-line amplifiers	Aging

Fiber or cable cuts	Human error
Whole equipment	Power supply failure Software failure
Entire node	Power Failure Natural disasters

A study by Labovitz et al. that investigated Internet failures between November 1997 and November 1998 [LAB99], that resulted from such causes as power outage, maintenance upgrade, fiber cuts, and hardware problems. The percentage breakdown of each cause is shown in Fig. A.1.

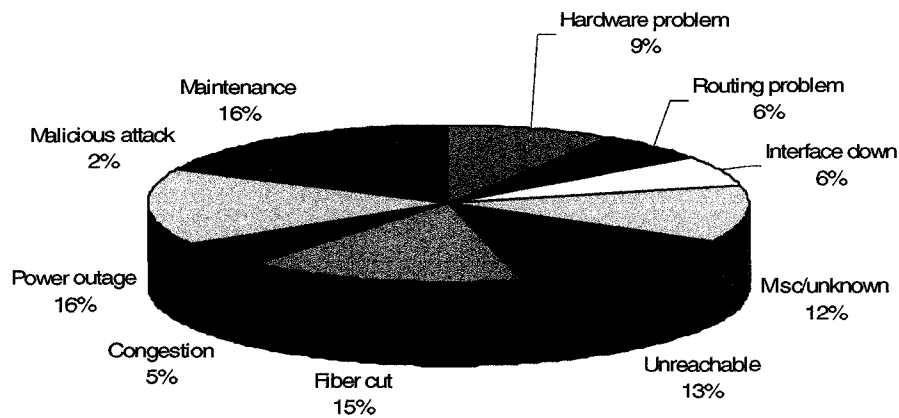


Fig. A.1: Causes of Network Failure [LAB99]

Network level failures may be classified according to its occurrence, which is very important for the network survivability analyzes, to the following:

- Single vs. multiple failures,
- Sudden vs. progressive failure.

The majority of the network survivability schemes have protection capability against single failure and a small number has it for multiple failures. Few of those who have multi-layer survivability techniques are designed for that purpose.

From the network's point of view, any consequent triggered events due to a single failure in all of the layers will be counted as a multiple failures. E.g., a cable cut may produce a double failure in the IP/OTN network. It has to be noticed that the repair time for some of those faults may be relatively long, so we don't have to neglect its accordance probability especially in the large-scale networks.

Aging is a main reason for equipment failures, and the many cases it is progressive phenomena. Single degradation alarms have to be introduced for those cases, e.g. the optical power output of the transponders need to be monitored and an alarm signal would be generated if it's below a certain assigned level.

The survivability actions have to be different from those is due to sudden failures to the progressive ones. However, the use of hold-off delays when multiple alarms are forwarded to a given layer to decide whether to switch or not can make a difference between the abrupt and progressive cases.

Table A.2 provides the two different classifications for the previously listed faults.

Table A.2: Classification of Failures

Failure	Single (S) or Multiple (M)	Sudden (S) or Progressive (P)
Router interface cards	S	S, P
In-site connections	S, M	S
OTN terminal equipment' optical amplifiers	S	S, P
OTN MUX/DEMUX	S	S, P
Transponders	S, M	S, P
In-line amplifiers	S	S
Fiber or cable cuts	S	S

A.1. Failure Impact on the Service Layers

The faults in the network level affect the running services which may lead to either service disruptions, or to uncertain state which the software applications may not recover. One cannot predict how the different software applications will recover from network faults especially when the restoration time is variable.

Probable impact of the restoration time on some services is illustrated in Table A.3.

Table A.3: Impact of Restoration Time on Services [KAW98C]

Restoration time	Impact on services
0 – 50 ms	Service “hit”
50 – 200 ms	Potential voice-band disconnects < 5% Cell/packet re-routing process affected
200 ms – 2 s	Voice-band call dropped
2 – 10 s	All circuit switched services dropped Private line disconnects Potential data session times out
10 s – 5 min	X.25 packet disconnects Data session times out
5 min – 30 min	Network congestion, public / business crashes
> 30 min	Major public / business crashes

Fig. A.2 classifies some classes of IP based services according to a certain allowable restoration time. Although the restoration time for the real time applications is very short, it causes service disruptions while longer restoration times in the non-real time applications can be tolerated.

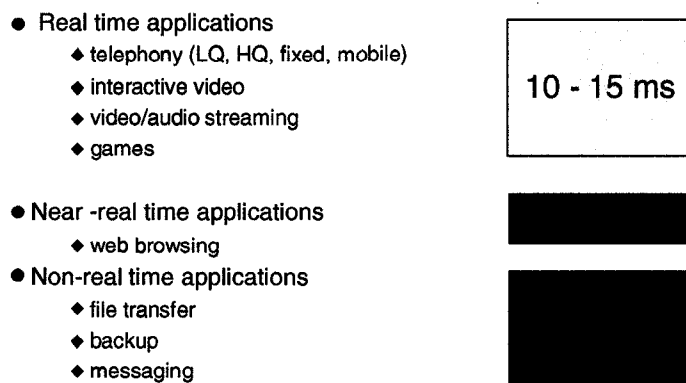


Fig. A.2: Impact of Restoration Time on some IP-based Services

A.2. Single-layer Network Survivability Measure

Protection uses a pre-assigned capacity, and that use is subject to a measure. The Quality of Protection (QoP) and the Priority Classes can be used as a survivability measure.

A.2.1. Quality of Protection (QoP)

Quality of Protection (QoP) is one aspect of the quality of service (QoS) that is suitable for reliable IP over OTN networks [ANSI01]. The implementation of QoP has been considered by several research groups:

- One suggested way is to split the primary lightpath into several segments.
- Another way to provide QoP is to use the differentiated reliability (DiR) of a connection. This is the maximum probability that the connection will fail due to a single network component failing.

The three QoP classes are:

- Class 1: Provides both primary and backup lightpaths if wavelengths are available.

- Class 2: Provides a backup path, but it can be taken by a primary lightpath with the above QoP Class 1 if a wavelength is not available.
- Class 3: Provides only primary lightpaths; no protection mechanism is provided.

A.2.2. Priority Classes

Combinations of both available classes of protection and restoration schemes can form certain network survivability policies that can be used to implement a network that can realize client service requirements.

The realization of these network survivability policies has to consider the different possibilities of the grades of service in terms of the restoration efficiency or the amount of restored traffic and the recovery response, and this forms what can be called survivability priority classes. The restoration efficiency may vary from 100% to 50%, 25%, or 0%. On the other hand, the recovery time can be 50 ms, 200 ms, 1 min, or no guaranteed time. Any category of class has to guarantee that the offered performance will be the worst case and that the user will expect a better one (if it is available).

Restoration efficiency depends on the scheme used for protection (e.g. 1+1, 1:1, or $m : n$), and for restoration of the network resources available at the recovery period as well as the routing techniques used.

Recovery time, on the other hand, depends mainly on the survivability schemes used, i.e. the fast response of the failure detection as well as the efficiency of the algorithms and protocols used. The recovery time is typically 50 ms in the case of protection

schemes with high priority classes, and lower than that for the others, while in the dynamic distributed restoration schemes, 200 ms is the average with 100% efficiency.

The different priority classes that may be offered to a customer are listed as following:

- **High priority class I: (100%, 50 ms) protection for path failures.** The user would have protection for all of his traffic and the recovery time will be within the SONET time limit, for either single or multiple link and node failures within the same path (excluding terminal node failures). Examples in the optical layer are the networks implementing either 1+1 OMS or OCh automatic protection.
- **High priority class II: (100%, 50 ms) protection for single link failure.** The user would have protection for all of his traffic and the recovery time will be within the SONET time limit for only single link failures.
- **Medium priority class I: (50%, 50 ms).** The user would have protection for 50% of his traffic and the recovery time will be within the SONET time limit, for either single or multiple link and node failures within the same path (excluding terminal node failures).
- **Medium priority class II: (50%, 50 ms).** The user would have protection for 50% of his traffic and the recovery time will be within the SONET time limit, for only single link failures.
- **Low priority class: (50%, 1 min).** The user would have protection for 50% of his traffic and the recovery time will not exceed 1 min with the limit of

200 ms provided by dynamic distributed restoration schemes, for single link failure only.

- **No protection.**

In network planning, parameters like the number of priority classes provided and their type are important and sometimes critical for the network administrator to fulfill the customers' entire request.

An example of the priority classes implemented in the optical layer may be deployed if the customer traffic required is High Priority Class I. In this case we do not have any choice but to use OMS 1+1 or OCh automatic protection.

Appendix B: Survivability Analysis in the Network Transport Layers

B.1. Optical Layer

The optical layer can be divided into three sub-layers. This division is described in the ITU-T G.872 Recommendation. The three sub-layers are:

1. The Optical Channel sub-layer (OCh),
2. The Optical Multiplex Section sub-layer (OMS), and
3. The Optical Transmission Section sub-layer (OTS).

These layers are shown in Fig. B.1 and Table B.1,

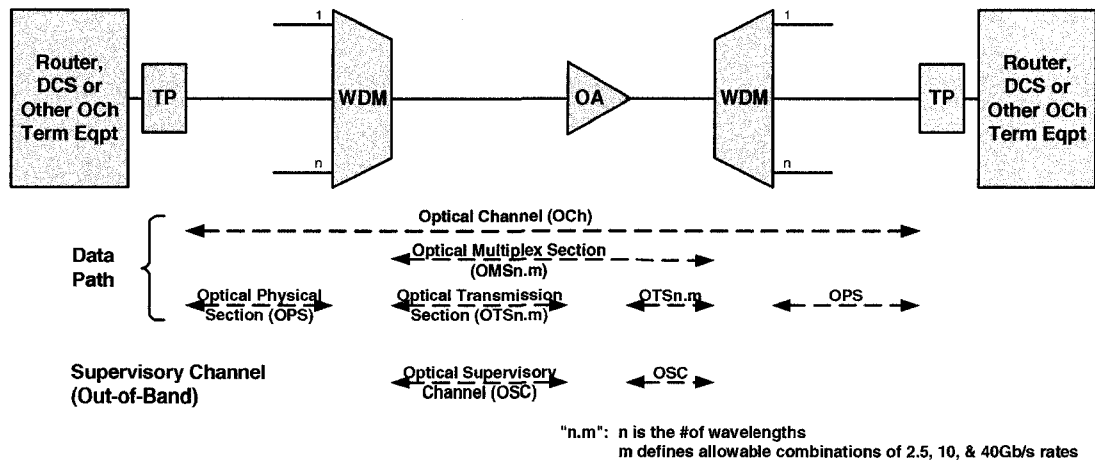


Fig. B.1: Optical Sub-layers

Table B.1: Optical Sub-layers [MAL02]

Electronic Layers	
OTN	OCh-Optical Channel
	OMS-Optical Multiplex Section
	OTS-Optical Transmission Section
	Physical media (optical fiber)

The Optical Transport Module OTM according to ITU-T G709 is illustrated in Fig.

B.2.

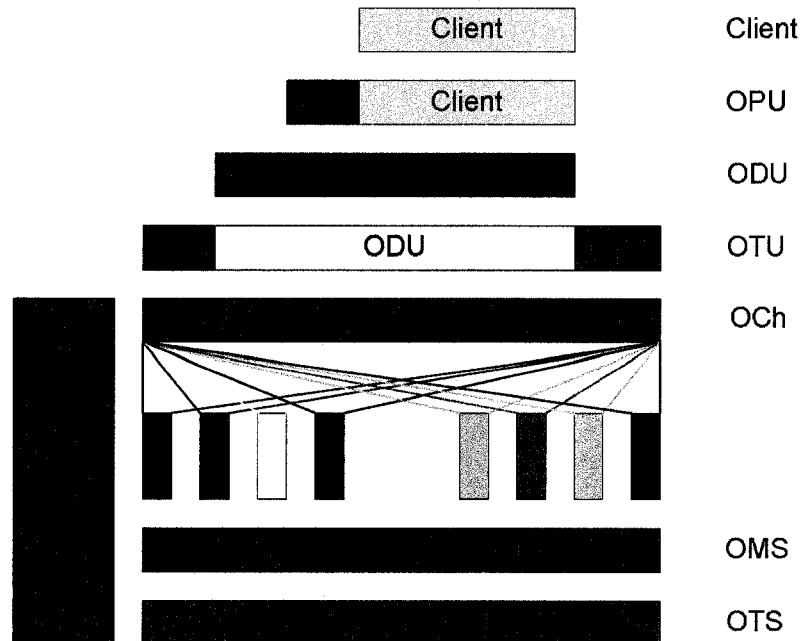


Fig. B.2: Optical Sub-layers [ITU03A]

To achieve management functionality, overhead is added to the client signal that, together with the FEC, forms the Optical Transport Unit (out).

The OTU is carried by a single wavelength as an Optical Channel (OCh) (as shown in Fig. B.3) and is transmitted as illustrated in Fig. B.4.

Adding OH via the Optical Supervisory Channel (OSC), the OMS and the OTS are formed.

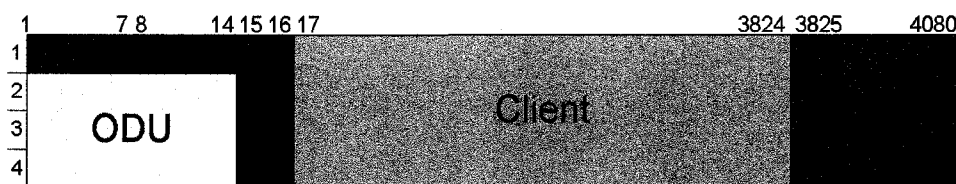


Fig. B.3: Optical Channel OCh [ITU03A]

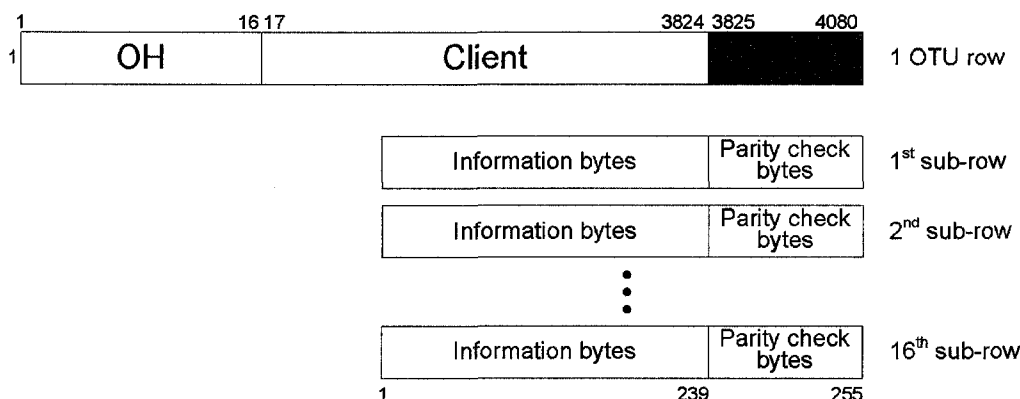


Fig. B.4: OTU Transmission [ITU03A]

The OTU row is split into 16 sub-rows (code word) each consisting of 255 bytes. The sub-rows are formed bytes interleaved. 239 bytes of the sub-row are used to calculate the FEC parity check, the result of which is transmitted in bytes (symbols) 240 to 255 of the same sub-row.

Frame Alignment Signal FAS is used for synchronization.

Optical Channel Transport Unit OTU overhead which consists of sub fields for the path monitoring OH (with the exception to the Incoming Alignment Error IAE bit); Section Monitoring SM, which provides monitoring functions and supports transport between 3R regenerators, and General Communication Channels GCC, those two fields allow communication between section end points.

Optical Channel Data Unit ODU overhead allows the user to support Tandem Connection Monitoring TCM (as shown in Table B.2) which enables signal management across multiple networks, Path Monitoring PM (as shown in Table B.3) which enables the monitoring of particular sections within the network and fault location, Automatic Protection Switching and Protection Communication Channel APS/PCC which provides APS switching on one or more levels, however these four bytes are currently undefined, and Fault Type (as shown in Table B.4) and Fault Location Channel FTL, a 256 byte multi-frame signal providing fault status information regarding type and location of the fault.

Table B.2: TCM Status Interpretation [ITU03A]

TCM byte 3, bits 6,7&8	Status
000	No source TC
001	In use without IAE
010	In use with IAE
011	Reserved
100	Reserved
101	Locked Defect LCK maintenance signal
110	Open Connection Identification OCI maintenance signal

Table B.3: PM Status Interpretation [ITU03A]

PM byte 3, bits 6,7&8	Status
000	Reserved
001	Normal path signal
010	Reserved
011	Reserved
100	Reserved
101	Locked Defect LCK maintenance signal

110	Open Connection Identification OCI maintenance signal
111	Alarm Indication Signal AIS maintenance signal

Table B.4: Fault Indication Codes Interpretation [ITU03A]

Fault Indication Codes	Definition
0000 0000	No Fault
0000 0001	Signal Fail
0000 0010	Signal Degrade
0000 0011	Reserved
.	
.	
1111 1111	

Optical Channel Payload Unit OPU overhead regulates the mapping and concatenation of the client signals and provides information on the type of signal transported (as shown in Table B.5).

Table B.5: Payload Type Code Points [ITU03A]

Hex code	Interpretation
01	Experimental mapping
02	Asynchronous STS-N mapping
03	Bit synchronous STS-N mapping
04	ATM mapping
05	GFP mapping
06	Virtual Concatenated signal
10	Bit stream with octet timing mapping
11	Bit stream without octet timing mapping
20	ODU multiplex structure
55	Not available
66	Not available

80-8F	Reserved codes for proprietary use
FD	NULL test signal mapping
FE	PRBS test signal mapping
FF	Not available

The optical sub-layers and its SONET equivalents are illustrated in table B.6.

Table B.6: Optical Sub-layers and its SONET Equivalents

OTN (ITU Terms)	SONET (rough equivalent)
OCh	Path
OMS	Line
OTS	Section

B.2. IP Layer

The survivability of the data transferred through the Internet is the result of the coordination between the routers and hosts. This kind of coordination is done by using routing protocols that are responsible for collecting, disseminating, and processing routing-related information.

B.2.1. IP Layer (OSI layer 3) Routing Protocols

The routing protocols perform network topology discovery and updating in case of the insertion of a new network element (node or link) into the network, or in case of network failure for any reason.

The survivability of IP networks depends mainly on routing protocols to detect the failure in the network and perform re-routing. The failure may be in one or multiple links.

Although the routing protocols can guarantee network survivability, they can not guarantee the recovery time, which depends on many factors like the topology itself and its complexity, its dimension, and the protocols used.

From the OSI layer's point of view; the IP layer is a client of the physical layer which performs the data transfer between the network nodes. And because there are no specific standards for how they exchange network information between them, we can say that the IP routing protocols are transparent in their activity to the physical layer regardless of its structure and shape.

The architecture of the Internet can be seen as a collection of separate domains that are called Autonomous Systems (AS). Each of these ASs contains groups of not necessarily identical routers connecting together to form another set of sub-networks.

An administrative authority that manages the AS does not have any constraint on the internal routing architecture provided that the routing information is available to the interconnected sub-networks routers. If the router is connected to other routers in the same AS, we call it an interior router. And if it is connected to other routers belonging to other ASs, we call it an exterior router.

Interior Gateway Protocol (IGP) is used to exchange the routing information between the interior routers, while Exterior Gateway Protocol (EGP) is used to exchange the routing information between the exterior routers.

B.2.1.1. Interior Gateway Protocols (IGP)

There are two types of protocols used as IGPs, the first uses distance-vector routing algorithm, while the second uses link-state routing algorithm. A comparison between distance-vector and link-state routing algorithms is listed in Table B.7.

Table B.7: A Comparison between Distance-vector and Link-state Routing Algorithms [BLA00]

Distance-Vector Routing	Link-State Routing
Each router sends routing information to its neighbors	Each router sends routing information to all other routers
The information sent is an estimate of its path cost to all networks	The information sent is the exact value of its link cost to adjacent networks
Information is sent on a regular basis	Information is sent when changes occur
A router determines next-hop information by using the distributed Bellman-Ford algorithm on the received estimated path costs	A router first builds up a description of the topology of the internet and then may use any routing algorithm to determine next-hop information

An example of a distance-vector routing algorithm is Routing Information Protocol (RIP), and for link-state routing algorithm is Open Shortest Path First protocol (OSPF). The RIP, because of its simplicity, is suitable for smaller ASs while OSPF is now considered the preferred interior routing protocol.

The advantage of OSPF over RIP concerning survivability can be summarized as follows:

- Faster in the reconfiguration time (takes shorter time than RIP),
- Provides multiple paths to the destination with different services.

B.2.1.2. Exterior Gateway Protocols (EGP)

The functions of Exterior Gateway Protocols EGPs are to perform the followings:

- Neighbor acquisition,
- Neighbor reachability,
- Network reachability.

Border Gateway Protocol BGP and Inter-Domain Routing Protocol IDRP are known types of Exterior Gateway Protocols EGPs. Both are using Path-Vector routing algorithm. The differences between Border Gateway Protocol BGP and Inter-Domain Routing Protocol IDRP are listed in Table B.8.

Table B.8: A Comparison between Border Gateway Protocol BGP and Inter-Domain Routing Protocol IDRP

Border Gateway Protocol BGP	Inter-Domain Routing Protocol IDRP
Operates only over TCP	Operates over any other internet protocol
Uses 16-bit AS number	Uses variable-length identifiers
Communicates a path by specifying the complete list of ASs that a path visits	Aggregate this information using the concept of routing domain confederation

B.3. SONET

SONET survivability has three known network schemes:

- 1) Protection switching: In this scheme, the p-p terminal equipment establishes a pre-assigned substitute connection without the assistance of the network management control functions.
- 2) Self-healing: In this scheme, the terminal equipment establishes a pre-assigned substitute connection without the assistance of the network management control functions.
- 3) Rerouting: In this scheme, the terminal equipment establishes a pre-assigned substitute connection without the assistance of the network management control functions.

SONET networks are subdivided into various layers (as shown in Fig. B.5 and Fig. B.6) that are directly related to the network topology.

Each layer of the SONET and network has its own overhead information. The transport modules (synchronous payload envelope), SPE are designated for carrying the payload. The payload may consist of various signals, each with a particular mapping.

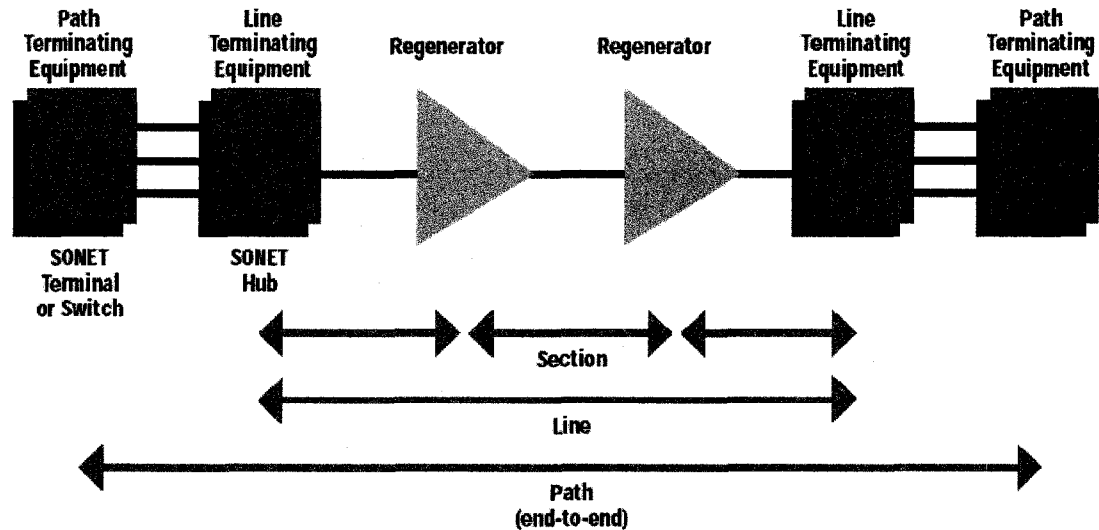


Fig. B.5: SONET Sub-layers

There are other possibilities for SONET transport networks, such as ATM, IP or ISDN, which can be mapped into SPE.

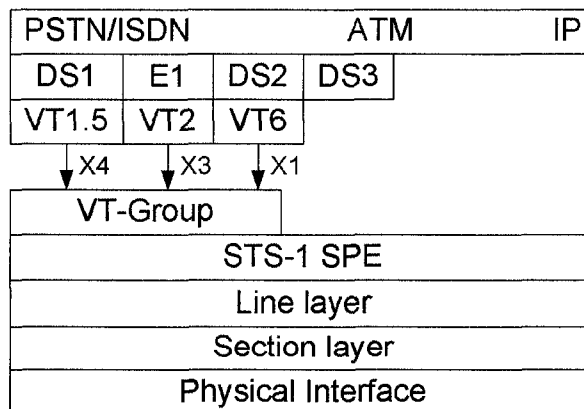


Fig. B.6: SONET Layer Model [NAT03]

Fig. B.7 shows the format of the base transmission in SONET which is called the Synchronous Transport Signal STS-1. Its Transport Overhead TOH, Path Overhead and Virtual Tributary Path Overhead VT-OH are illustrated in Fig. B.8. Table B.9 lists STS-1 Header Information.

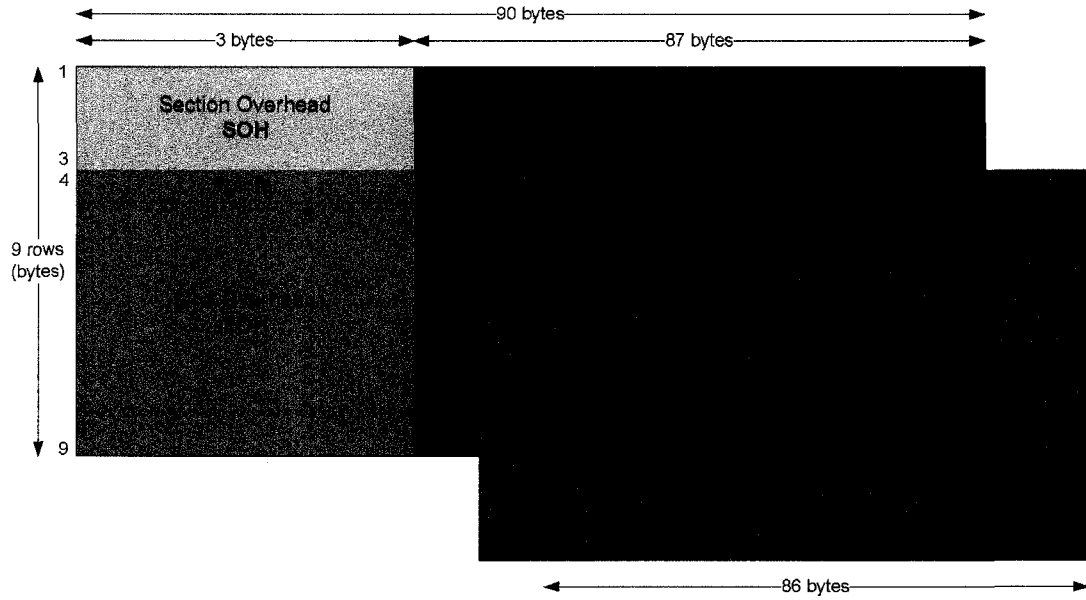


Fig. B.7: STS-1 Frame Structure

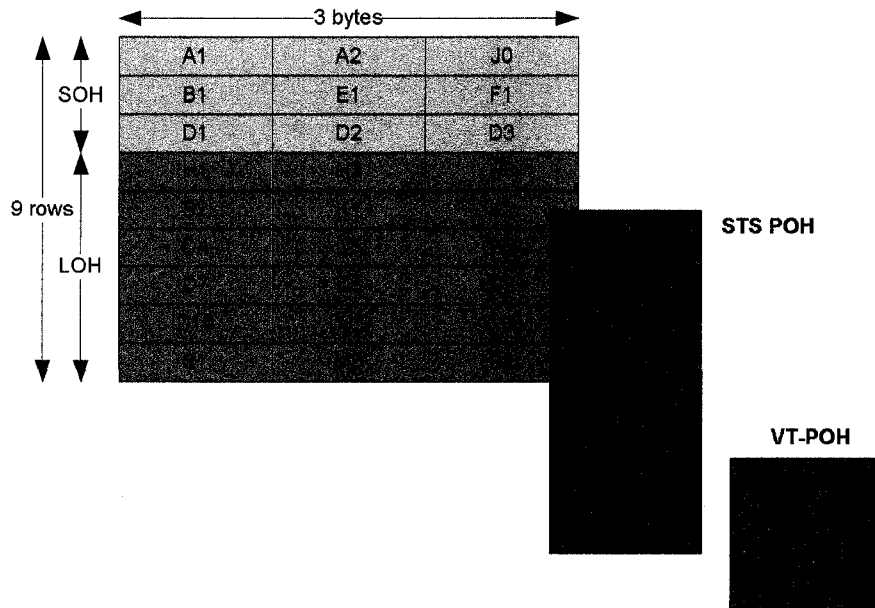


Fig. B.8: STS-1 TOH & POH

Table B.9: STS-1 Header Information

Header	Function
A1,A2	Framing
AU Pointer	Administrative Unit Pointers
B1,B3	BIP-8 (Bit Interleaved Parity)
B2	BIP-24
C1,C2	STS-1 Identifier
D1 to D12	Data Communication channels
E1,E2	Order Wire
F1,F2	User-defined channels
G1	Path Status
H4	Multi-frame Indicator
J1	Path Trace
K1,K2	Automatic Protection Switching
Z1 to Z5	Reserved

In the LOH, there are two bytes “K1” and “K2” are used on the protection line for Automatic Protection Switching APS signaling. This is for line level protection switch. Table B.10 lists SONET K1 & K2 messages as specified in ANSI T1.105.01 [ANSI01].

Table B.10: SONET K1 & K2 Messages

K1 byte	b1 – b4	Linear APS Messages	Ring APS Messages
		Lockout of protection	Lockout of protection (span) or signal fail (protection)
	1110	Forced switch	Forced switch (span)
	1101	Signal fail high priority	Forced switch (ring)
	1100	Signal fail low priority	Signal fail (span)
	1011	Signal degrade high priority	Signal fail (ring)

	1010	Signal degrade low priority	Signal degrade (protection)
	1001	Unused	Signal degrade (span)
	1000	Manual switch	Signal degrade (ring)
	0111	Unused	Manual switch (span)
	0110	Wait-to-restore	Manual switch (ring)
	0101	Unused	Wait-to-restore
	0100	Exercise	Exerciser (span)
	0011	Unused	Exerciser (ring)
	0010	Reserve request	Reserve request (span)
	0001	Do not revert	Reserve request (ring)
	0000	No request	No request
	b5 – b8	Selects channel used by APS messages	Destination node ID
K2 byte	b1 – b4	Selects bridged channel used	Source node ID
	b5	Determines automatic protection switch architecture	Path code: 0 = short path; 1 = long path
	b6 – b8		
	000	Reserved	Idle
	001	Reserved	Bridged
	010	Reserved	Bridged and switched
	011	Reserved	Extra traffic (ET) on protection channels
	100	Provisional mode is unidirectional	Reserved
	101	Provisional mode is bidirectional	Reserved
	110	RDI-L	RDI-L
	111	AIS-L	AIS-L

B.4. ATM

At ATM, the VP has some unique characteristics. The most striking characteristic is the independence of route and bandwidth establishment, allowing a VP route to be established without assigning its bandwidth along the path. This is not the case in SONET networks, in which a digital path is established by assigning a time slot of the STS frame to each cross-connect on the path, allowing only fixed bandwidth digital paths to be established.

The ATM protocol reference model, defined in ITU-T recommendation I-321, is shown in Fig. B.9. Table B.11 summarizes the functions of each layer. Fig. B.10 shows different ATM cell formats.

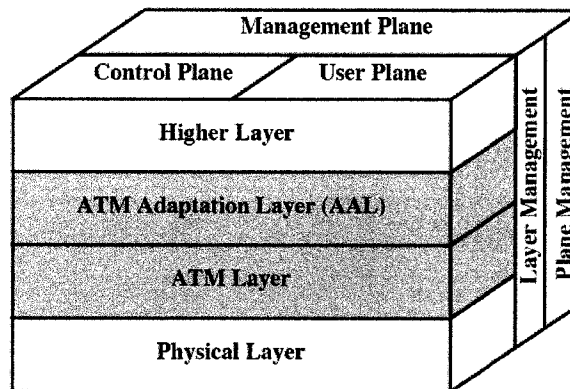


Fig. B.9: ATM Protocol Architecture [STA02]

Table B.11: Summarization the ATM Layers Functions

Layer Management	Higher Layer Functions	Higher Layers	
	Convergence	CS (Convergence Sublayer)	AAL (ATM Adaptation Layer)
	Segmentation and reassembly	SAR (Segmentation)	

And

		Reassembly)	
	<i>Generic flow control</i> <i>Cell-header generation/</i> <i>extraction</i> <i>Cell VPI/VCI translation</i> <i>Cell multiplex and</i> <i>demultiplex</i>	ATM layer	
	<i>Cell-rate decoupling</i> <i>HEC, header-sequence</i> <i>Generation/verification</i> <i>Cell delineation</i> <i>Transmission-frame</i> <i>adaptation</i> <i>Transmission-frame</i> <i>generation/recovery</i>	TC (Transmission Control)	PHY Independent
	<i>Bit timing</i> <i>Physical medium</i>	PM (Physical Medium)	PHY Dependent

The ATM connection includes Virtual Channel Connection (VCC) and Virtual Path Connection (VPC), and connection segment hierarchy is illustrated in Fig. B.11 [AND97B].

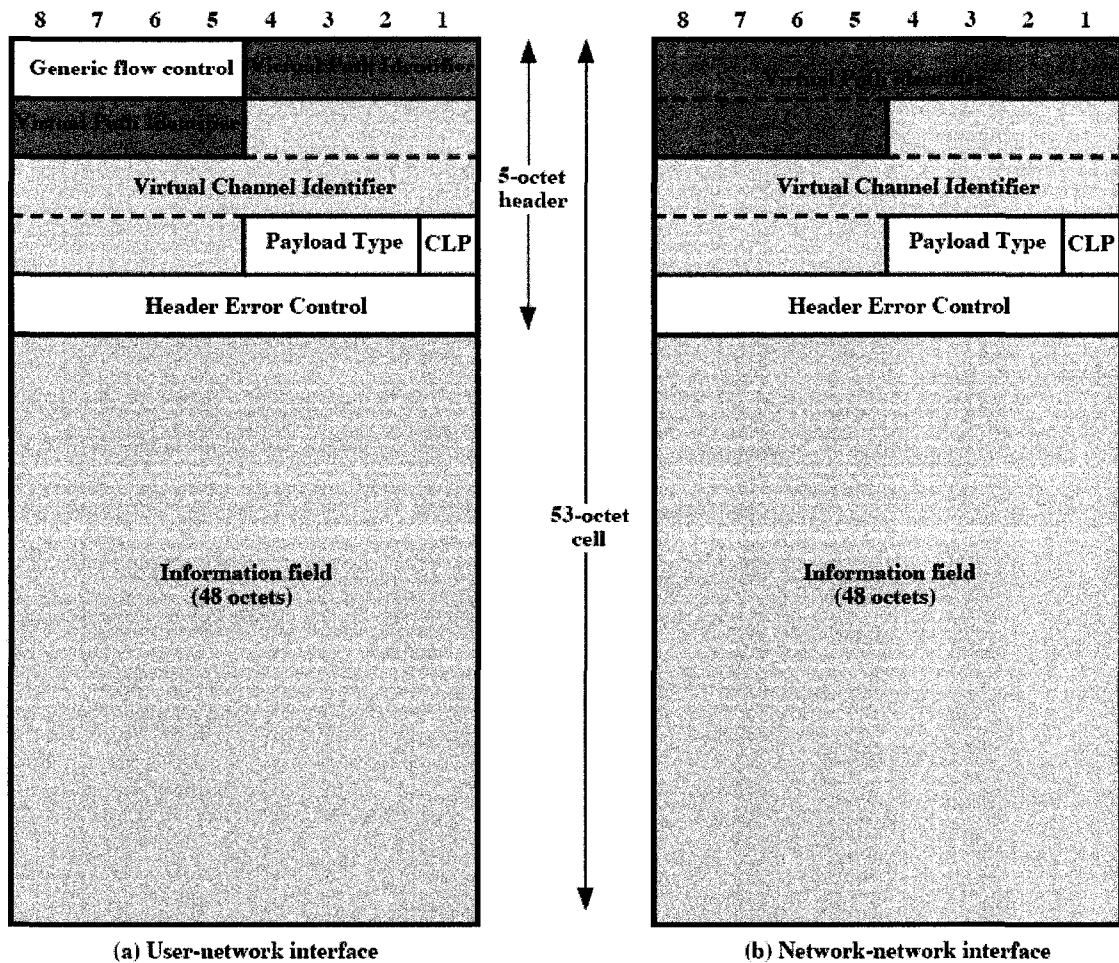


Fig. B.10: ATM Cell Format [STA02]

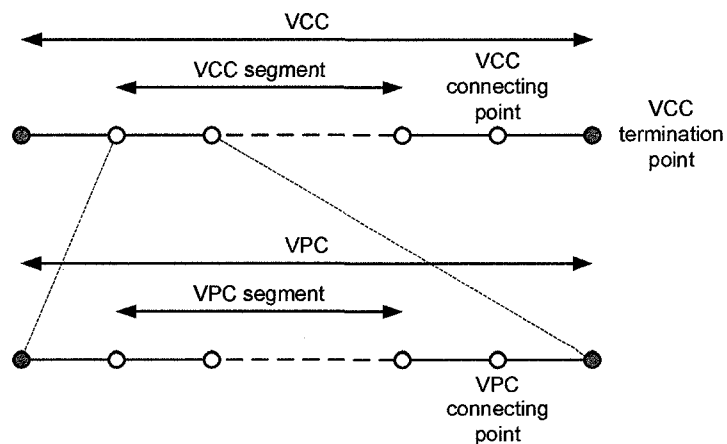


Fig. B.11: ATM Connection and Connection Segment Hierarchy [AND97B]

In the normal operating mode, when the ATM terminal receives a call to establish VCC, it checks whether its QoS requirements are satisfied before making the connection,. Fig. B.12 demonstrates the process block diagram.

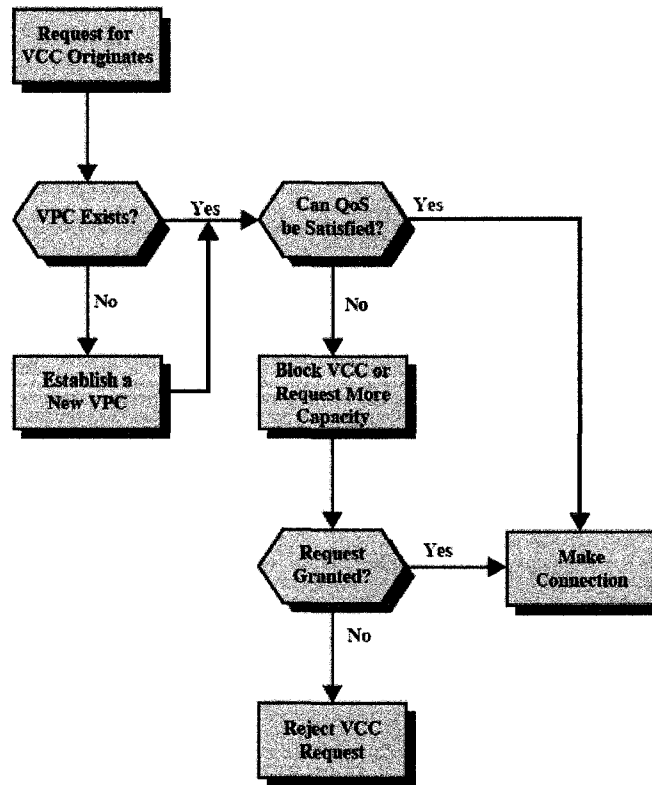


Fig. B.12: Call Establishment Using Virtual Paths [STA02]

Messages are exchanged between the calling end-station and its nearest neighbor. These messages are passed along the network until the called party is reached and can acknowledge the call. This is illustrated in Fig. B.13.

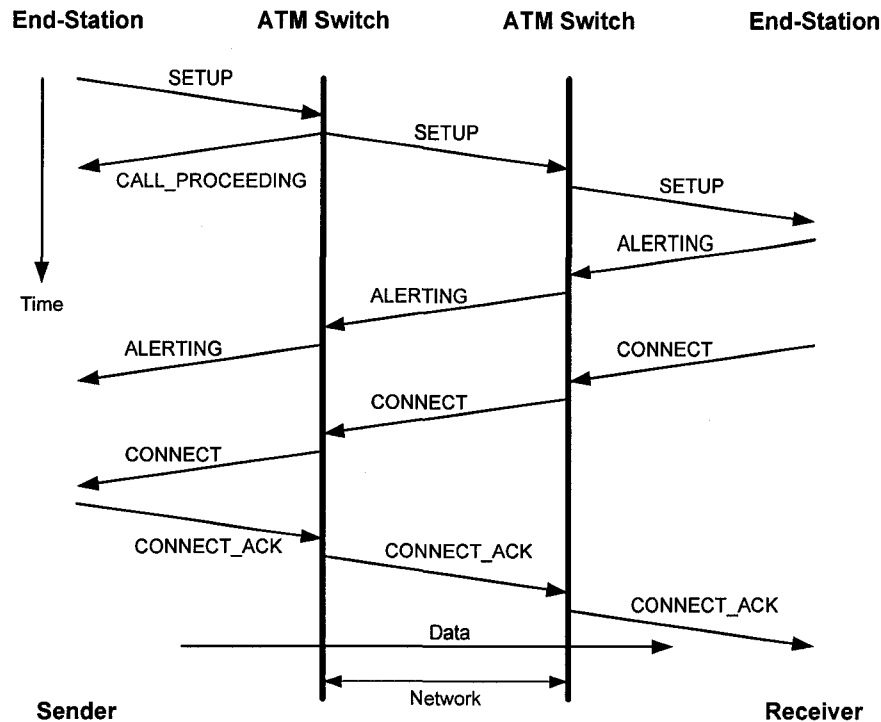


Fig. B.13: ATM Terminal Messages Exchange

B.4.1. Survivable ATM Network Management Architecture

In order to meet with the required QoS, the ATM network resource management requires complicated procedures to do resource allocation requests from several levels of traffic entities (i.e ATM cells, calls and virtual paths). A layered switching architecture has been proposed for ATM networks to reduce such complexity. The network manager at each level focuses on the resource allocation of its layer's traffic to fulfill the QoS. The four layers of this survivable ATM network management architecture are illustrated in Fig. B.14 [MUR97].

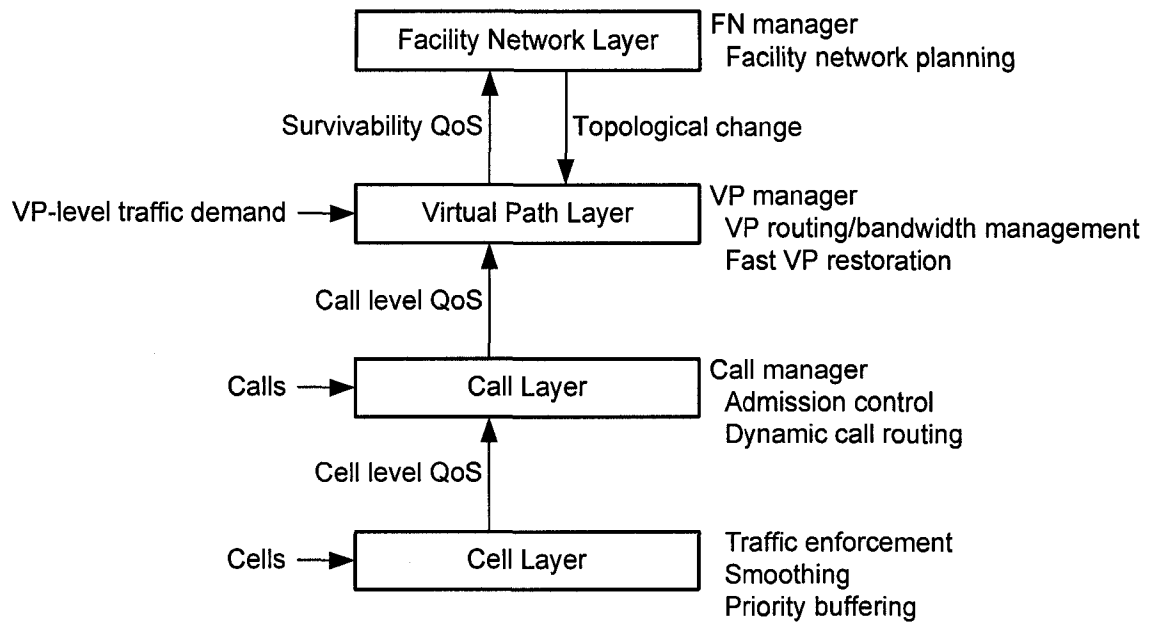


Fig. B.14: ATM Survivable ATM Network Management Architecture [MUR97]

The survivability functions are set up at the VP and FN layers because recovery at the path level allows for fast and efficient restoration and significantly decreases the complexity of traffic management.

Because of this hierarchy, if a network failure happens, the VP manager starts to perform the restoration, and if he cannot for any reason, the FN has to initiate a facility network planning process [MUR97].

B.4.2. Operation Administration and Maintenance (OAM) Cell

The ATM uses Operation Administration and Maintenance OAM cell for fast and reliable message transmission between network elements (NEs). Its significant use is in the restoration schemes [AND94A]. Table B.12 summarize ITU-T 1.610 ATM-layer OAM functionality [AND97B].

Table B.12: Summary of ITU-T 1.610 ATM-layer OAM Functionality [AND97B]

OAM Cell Type	Function Type	Main Application	Conveyed Information
Fault management (FM)	Alarm indication signal (AIS)	Reporting defect indications in the forward direction	Detected defect type and location ID
	Remote defect indication (RDI)	Reporting remote defect indications in the backward direction	Detected defect type and location ID
	Continuity check (CC)	Continuous monitoring of connection continuity	None defined
	Loop back	• Fault localization • On-demand connectivity monitoring • Pre-service connectivity verification	Information to control the cell loop back, such as source and loop back point IDs and loop back correlation tag
Performance management (PM)	Forward monitoring (FM)	Measuring performance in the forward direction	Information to provide estimates of cell loss and cell misinsertion ratios, cell block error, cell transfer delay, and delay variation per connection

	Backward reporting (BR)	Reporting performance measurements in the backward direction	Report of information to source point to provide estimates of performance measured in the forward direction
OAM activation and deactivation	PM forward monitoring	Activating or deactivating OAM	Information to control setup or release of the PM function, such as PM block size
	PM backward		
	FM continuity check		Information to control setup or release of the CC function
System management	None specified	For use by end-systems only	None defined

An ATM OAM cell is illustrated in Fig. B.15 according to ITU-T I.610.

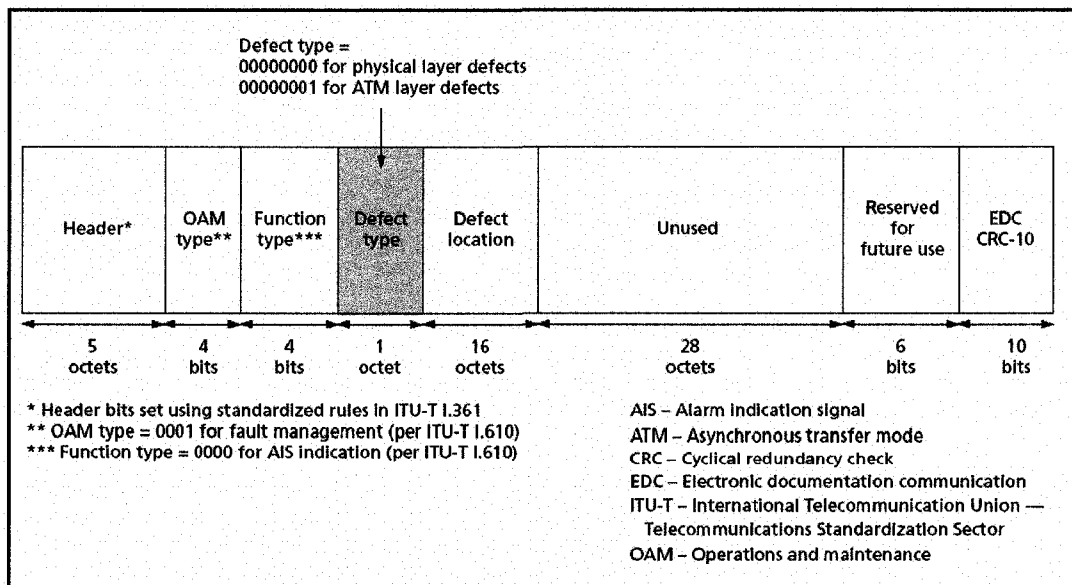


Fig. B.15: ATM OAM Fault Management Cell with Defect Type Indicator [AND97B]

A failure management scheme for the VP layer using OAM cells is illustrated in Fig. B.16 [AND97B]. After the failure detection, VP-AIS cells are propagated and transmitted periodically (every second). As soon as the near-end VP termination point receives the VP-AIS, it declares its state and sends a VP-RDI cell to the far end. This triggers the restoration schemes. Cross-connect nodes along the failed VP accordingly detect the failure very quickly. ITU-T SG13 is working to enhance the restoration mechanism and address the inter-domain issues.

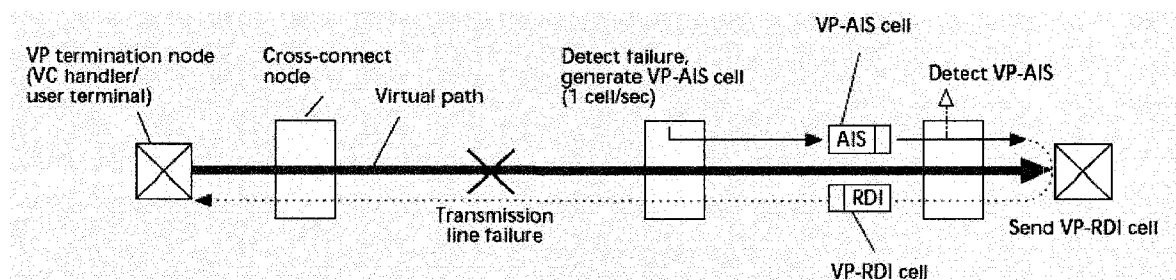


Fig. B.16: Alarm Transmission Mechanism for VP Layer [KAW98C]

B.5. MPLS (GMPLS)

MPLS as a new backbone technology must provide satisfactory service for the network traffic, including the protection of the traffic carried on the LSPs. MPLS protection switching refers to the capability of the MPLS layer to rapidly and fully restore traffic during any changes in the condition of the MPLS layer. Fast MPLS layer protection should be as good as the 50 ms restoration time of the SONET layer.

MPLS's re-routing layer solves a lot of problems and provides enhancements to the other existing layers, e.g.:

- It speeds up the re-routing in the IP layer which is otherwise very slow (measured in seconds).

- It provides a higher layer protection to some parts of the network where there are Optical and SONET layers limited to ring topologies and may not include mesh protection.
- It offers a fine protection granularity and facilitates different services between the different types of traffic that are protected.

B.5.1. MPLS Principles

At the ingress LSR (Label Switch Router), IP packets ingoing into a MPLS network are mapped to an explicit FEC (Forwarding Equivalence Class) as in Fig. B.17. A FEC is a group of L3 (layer 3) packets that require the same forwarding treatment (e.g. destination, QoS). The ingress LSR then gives a label to the packet based on its FEC and forwards it to the next hop in the label switched path (LSP). An LSP is seen as a virtual circuit which defines an ingress-to-egress path through the network with a specific FEC.

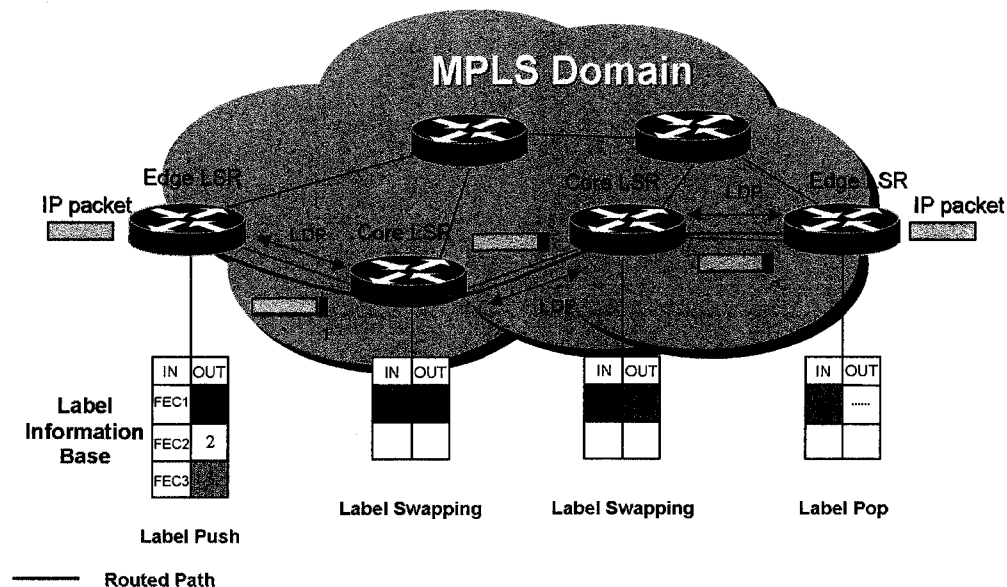


Fig. B.17: MPLS in Action: Simple Label-swapping and Forwarding in the Core

B.5.2. Multi-Protocol Lambda Switching

IETF designed the control planes for optical cross-connects (OXC) based on an extension of the MPLS Traffic Engineering control plane model that is called Multi-Protocol Lambda Switching (MP λ S), and its generalized version GMPLS. Such a control plane would be used to:

- Distribute information regarding the topology and the state of the optical transport network,
- Set-up optical channel trails,
- Support various traffic engineering functions in the optical domain,
- Enable a variety of protection and restoration capabilities,
- Simplifies the integration of OXC and label switching routers,
- Provide coherent semantics for network management and operations control in hybrid optical internetworking systems consisting of LSRs and OXC.

An option is to use a single instance of the control plane that considers and spans LSRs and OXC. In this case an LSP can pass through a mix of LSRs and OXC, or could pass only LSRs, or only OXC. This creates a possibility for LSRs to dynamically request bandwidth services from the optical network. Fig. B.18 illustrates a candidate OXC system architecture.

The main requirements for the OXC control plane are:

- The ability to establish optical channel trails expeditiously (in seconds or even milliseconds rather than days or months),
- The ability to support traffic engineering functions,
- The ability to support various protection and restoration schemes.

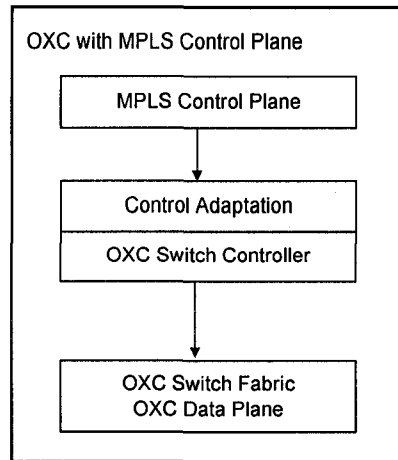


Fig. B.18: Candidate OXC Systems Architecture

B.5.3. MPLS Routing Protocols

The initial MPLS effort is focused on IPv4, so that IP routing protocols are used for path finding. MPLS also offers an option for Traffic Engineering. Extensions to the existing routing protocols such as OSPF-TE and ISIS-TE have been made. The optical extensions to the OSPF-TE to support GMPLS can be summarized into the following two categories: TE Link advertisements and Routing enhancements.

B.5.4. MPLS Signaling Protocols

RSVP-TE is used to establish MPLS LSPs when there are traffic engineering requirements. It is mainly used to offer QoS and load balancing across the network core, and includes the skills to control all-optical networks.

RSVP allows the use of source routing where the ingress router establishes the complete path throughout the network. The ingress router can use a Constrained Shortest Path First (CSPF) estimator to find out a path to the destination, ensuring

that any QoS and Shared Risk Link Group (SRLG) requirements are fulfilled. The resulting path is then used to establish the LSP.

The RSVP optical extensions are able to signal optical wavelengths and shared risk link groups, as well as bandwidth, latency and other link characteristics.

Label Distribution Protocol (LDP) is commonly used to set up MPLS LSPs when traffic engineering is not required. It establishes LSPs that follow the existing IP routing, and is mainly well suited for setting up a full mesh of LSPs between all of the routers on the network.

LDP can work in many modes to suit different requirements; however the most frequently used is unsolicited mode, which sets up a full mesh of tunnels between routers:

- In solicited mode, the ingress router sends an LDP label request to the next hop router, as found out from its IP routing table. This request is forwarded on throughout the network hop-by-hop by each router. Once the request arrives at the egress router, a return message is created. This message confirms the LSP and tells each router the label mapping to employ on each link for that LSP.
- In unsolicited mode, the egress routers broadcast label mappings for every external link to all of their neighbors. These broadcasts are disseminated across every link through the network until they reach the ingress routers. Across each hop, they notify the upstream router of the label mapping what to use for each external link, and by flooding the network they set up LSPs between all of the external links.

The main advantage of LDP over RSVP is the ease of setting up a full mesh of tunnels using unsolicited mode, so it is most frequently used in this mode to set up the underlying mesh of tunnels needed by MPLS-enabled VPNs.

Appendix C: Encapsulation Methods for the Different Network Architectures

C.1. IP/ATM/SONET/OTN Architecture

Fig. 3.2 shows an example for the Classical IP over ATM (RFC 1483) architecture; the IP packets are segmented into different Virtual Connections ATM cells IP router's ATM line-card interface. The ATM cells are either sent to an ATM switch or, after that, forwarded to SONET OADM where they are packed into a SONET frame and then to an OTN transponder for transport over the optical layer.

For the IP traffic (connection-less), ATM networks classify it as UBR (Unspecified Bit Rate) traffic contract and the AAL5 protocol is used as a transport facility.

The QoS of the IP service is maintained by using either one of the following two methods:

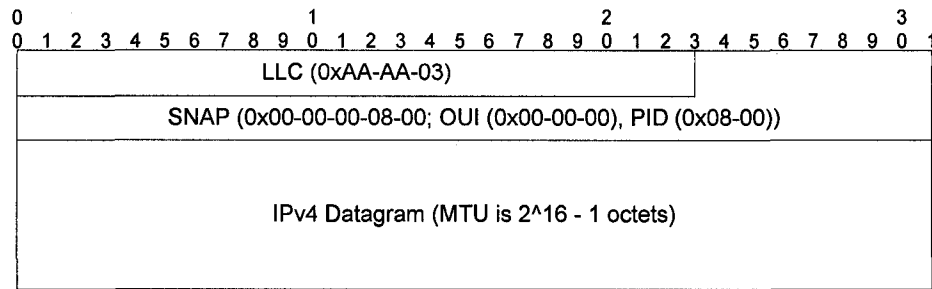
- 1) Permanent Virtual Channels (PVC) (layer 2 QoS management): the ATM management system do this by providing variable VC granularity which guarantees a fixed bandwidth between pairs of IP routers for each customer.
- 2) Switched Virtual Channels (SVC): the VC is dynamically set-up within Virtual Paths (VP). Statistical multiplexing can also be used to allow users to have extra bandwidth for short bursts.

The Payload field contains user information up to $2^{16} - 1$ octets. The PAD field (0 to 47 octets) pads the CPCS-PDU to fit exactly into the ATM cells such that the last

48 octet cell payload created by the SAR sub-layer will have the CPCS-PDU Trailer right justified in the cell. The protocol stack for this scenario is detailed in table C.1.

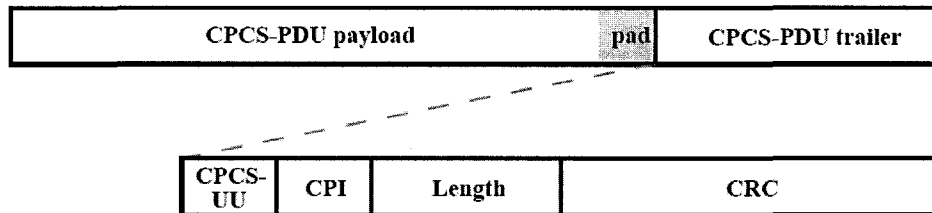
Table C.1: Protocol Stack for Classical IP over ATM over SONET

Layer/ sub-layer	Encapsulation method
IP	Packets up to $2^{16} - 1$ octets long to be encapsulated,
LLC/SNAP	Logical Link Control/ Sub-network Access Protocol (RFC 1483) adds 8 byte overhead to IP packet (as shown in Fig. C.1) to form ATM Common Part Convergence Sublayer- Protocol Data Unit (CPCS-PDU).
AAL5	ATM Adaptation Layer 5, (ITU-T I.363.5) adds CPCS-PDU trailer; 8 octets (CPCS-UU CPCS User-to-User indication; 1 octet, CPI Common Part Indicator; 1 octet, length; 2 octets, and CRC; 4 octets) (as shown in Fig. C.2). It also adds PAD field (0 to 47 octets) which pads the CPCS-PDU to fit exactly into an integral number of ATM.
ATM	The AAL5 CPCS PDU is segmented into 48 octet SAR-PDU payloads after that 5-octet overhead is added to every SAR-PDU payload to form 53 octet ATM cells (as shown in Fig. C.3).
SONET	The ATM cells are mapped into SONET STS-1 (as shown in Fig. C.4) or concatenated STS-3c payload (T1.105) (as shown in Fig. C.5). ATM frame is scrambled with a $x^7 + x^6 + 1$ polynomial in addition to payload scrambling with $1 + x^{43}$ polynomial to provide sufficient transition density for SONET clock recovery. The STS-1 or STS-3c may be multiplexed to form OC-48 or OC-192.
OTN	The SONET is carried by a certain wavelength (colored) and optically multiplexed into OTN fiber. Or the SONET is wrapped into OTN frame (ITU-T G.709) and carried by a certain wavelength (colored) and optically multiplexed into OTN fiber.



LLC = Logical Link Control
 SNAP = Subnetwork Access Protocol
 OUI = Organizationally Unique Identifier
 PID = Protocol Identifier

Fig. C.1: Adding LLC/SNAP Overhead to IP Datagram



CPCS-UU = CPCS user-to-user indication (1 octet)
 CPI = common part indicator (1 octet)
 Length = length of CPCS-PDU payload (2 octets)
 CRC = cyclic redundancy check (4 octets)

Fig. C.2: AAL Type 5 [STA02]

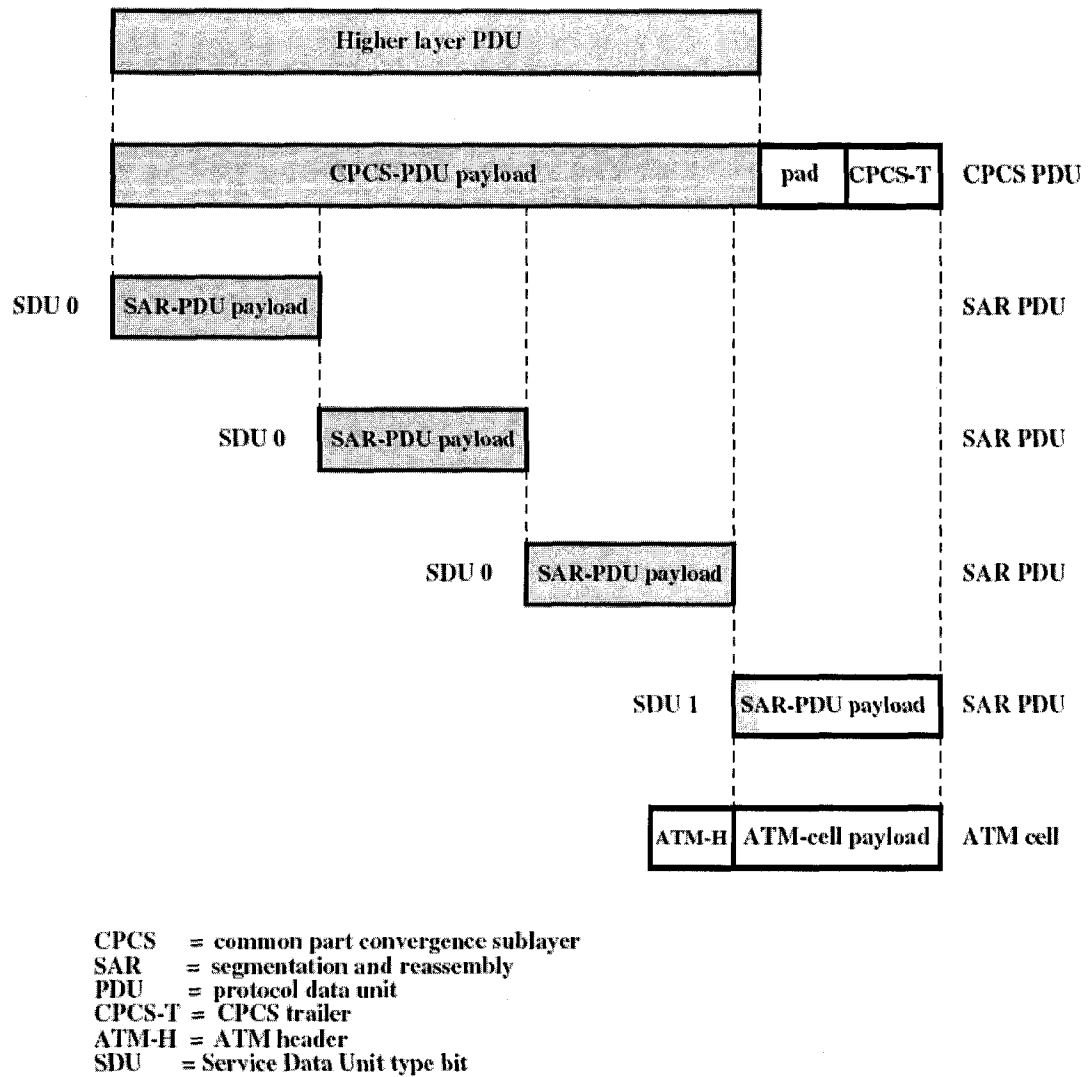


Fig. C.3: Example of AAL 5 Transmissions [STA02]



Fig. C.4: ATM Cell Mapping into a STS-1

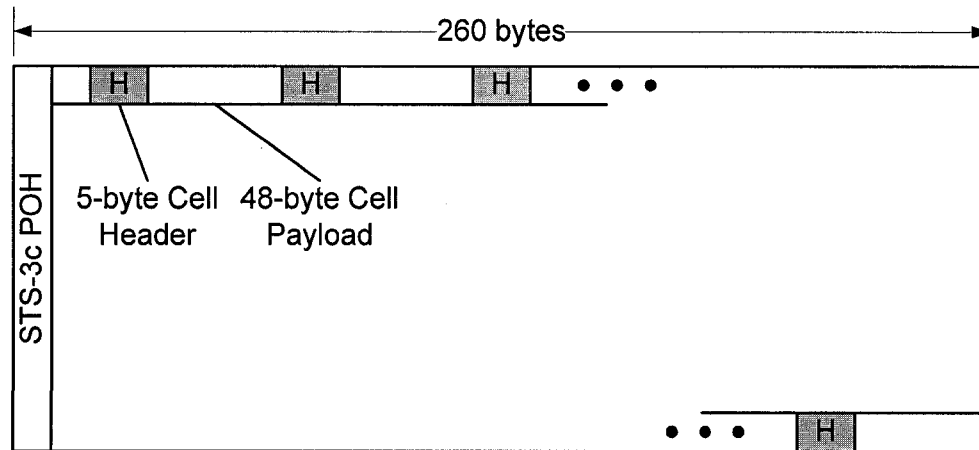


Fig. C.5: ATM Cell Mapping into a STS-3c

C.2. IP/SONET (POS)/OTN Architecture

The second network architecture scenario selected is IP over SONET over OTN. In general there are two possibility, as shown in Fig. 3.3 for IP over SONET; the first is simply by encapsulated IP packets into SONET formats and transmit it over OTN (by using a transponder), the second is encapsulated IP packets along with other traffic into SONET formats and transmit it over OTN links.

The most two common encapsulation methods for IP over SONET are:

- 1) POS or Packet over SONET (RFC 1619, RFC 1661, and RFC 1662) – as listed in Table C.2 and shown in Fig. C.6,
- 2) SDL over SONET (RFC 2823)

Table C.2: Protocols used for IP over SONET

Layer/ sub-layer	Encapsulation method
IP	Packets up to 65535 octets long to be encapsulated,
PPP	The IP datagram is PPP encapsulated (RFC 1661). Protocol field (IP, LCP, NCP); 2 octets (0x0021 for IP). Padding is optional at the end.

HDLC	The HDLC frame is used to delineation (framing) of the PPP packet (RFC 1662, 2615). The flag octet indicating frame starts (0x7E). Address field 0xFF (HDLC broadcast address). Control field is added (always 0x03 - unnumbered frame). 4 octets frame check sequence (FCS). Another flag octet indicating frame starts (0x7E). If a 0x7E occurs in the data, an escape sequence is used to replace 7E with 7D-5E, and any escape character 7D is replaced with 7D-5D (octet stuffing).
SONET	The HDLC frames are mapped into SONET STS-1 or concatenated STS-3c payload (RFC 1619). The payload scrambling with $1+x^{43}$ polynomial to provide sufficient transition density for SONET clock recovery. The STS-1 or STS-3c may be multiplexed to form OC-48 or OC-192.
OTN	The SONET is carried by a certain wavelength (colored) and optically multiplexed into OTN fiber. Or the SONET is wrapped into OTN frame (ITU-T G.709) and carried by a certain wavelength (colored) and optically multiplexed into OTN fiber.

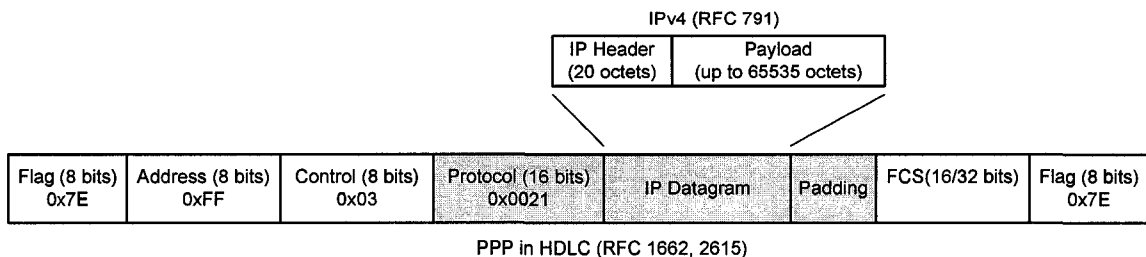


Fig. C.6: POS (Packet over SONET)

It is possible to simply use SONET formats to frame encapsulated IP packets for transmission over OTN, probably using a transponder (wavelength adapter), or it is also possible to transport the SONET -framed IP over an SONET transport network along with other traffic, which may then use OTN links.

The line-card in the IP router performs the PPP/HDLC framing. The optical signal is then suitable for transmission over optical fiber either into an SONET network

element, a neighboring IP router, or an OTN transponder for further transmission.

There are also different types of IP over SONET interfaces:

- OC3 or Concatenated OC3 “fat pipes” which provide aggregate bandwidth without any partitions between different IP services which may exist within the packet stream.
- Channelized interfaces, where an OC48 optical output may contain 16 individual OC3s, with a possible service separation for each OC3. The different OC3s can then also be routed by an SONET network to different destination routers.

The version of IP over SONET examined here uses PPP encapsulation and HDLC framing. PPP is a standardized way to encapsulate IP and other types of packets for transmission over many media from analogue phone lines to SONET, and also includes functionality to set up and close links (LCP). HDLC is the ISO-standardized version of SDLC, a protocol developed by IBM in the 1970s. The HDLC framing contains delimiting flag sequences at the start and end of the frame, and also has a CRC checksum field for error control.

In this scenario, the IP layer is the only layer with packet routing functionality. According to the POS standards, the IP packets are adapted to the transport in the SONET layer using the PPP protocol and an HDLC-like framing.

The SONET layer can be functionally decomposed in two further layers: the Path layer and the Section layer (including Multiplex Section and Regenerator Section layer). For this scenario two options are possible:

- 1) A real SONET network is present with both Path layer and Section layer functionality
- 2) SONET is present only in the router interfaces and therefore only some Section layer functionality is actually used.

In the first case, SONET can also perform path routing, through ADM or DXC equipment. This situation is generally applicable when an SONET network is used as a server for different client networks and IP is just one of these clients. In the second case, the role of SONET is just to provide point-to-point transport of IP packets between routers, therefore Section layer functionality is required, only, and SONET is confined within the router interfaces, without pure SONET equipment installed in the network. This situation is typical of a backbone network optimized for the transport of IP. In backbone IP networks, the whole SONET section is generally used to transport a single broadband payload through the use of a single N-concatenated OCs (OC3c or OC12c).

C.3. IP/GbE/OTN Architecture

The frame structure for Gigabit Ethernet is shown in Fig. C.7.

Preamble (7 Octets)	SFD (1 Octets)	DA (6 Octets)	SA (6 Octets)	Type/Length (2 Octets)	Data/ PAD (max length 1500 Octets)	FCS (4 Octets)	Extension
------------------------	-------------------	------------------	------------------	---------------------------	---------------------------------------	-------------------	-----------

Fig. C.7: Gigabit Ethernet Frame

The MTU of Gigabit Ethernet is 1500 bytes, and the use of 4K Jumbo frames is not approved by standard bodies. The Ethernet frame is encoded onto an optical carrier using 64B/66B or 8B/10B encoding in order to ensure a sufficient density of signal

transitions for clock recovery. The different Gigabit Ethernet sub-layers are shown in Fig. C.8.

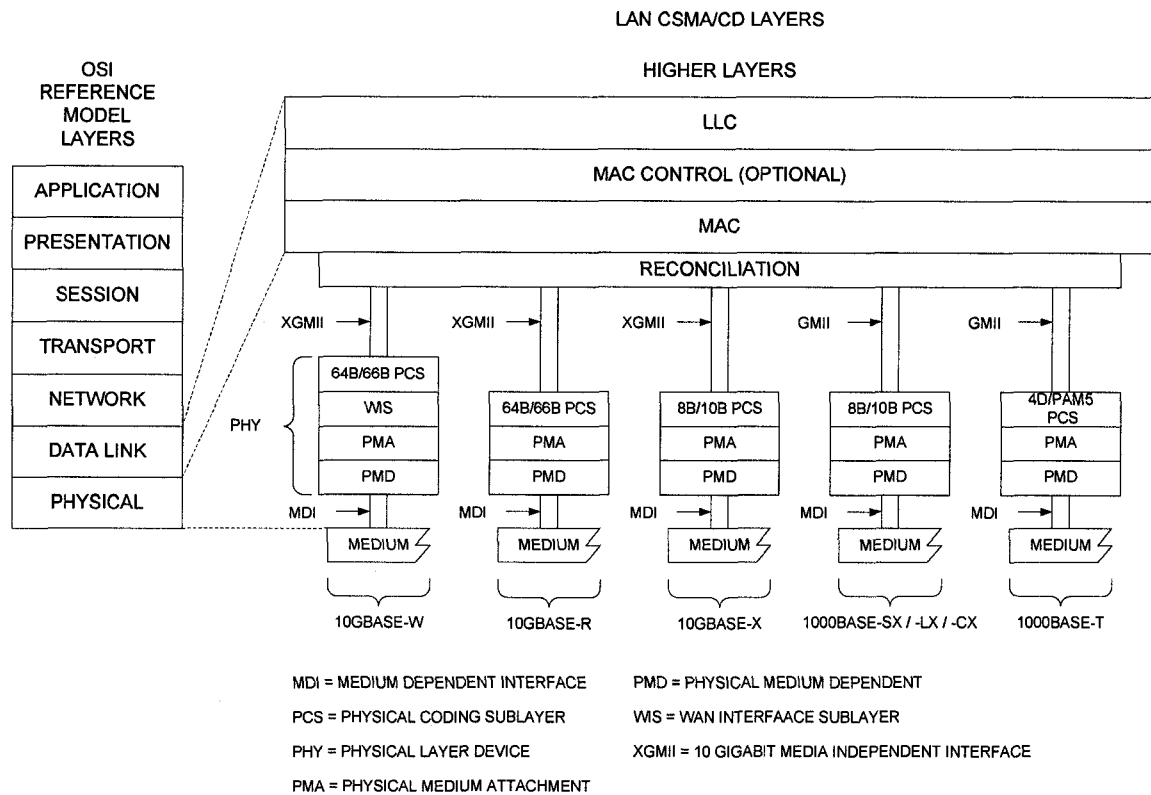


Fig. C.8: Gigabit Ethernet Sub-layers

Gigabit Ethernet provides QoS as specified in the standards IEEE 802.1Q and 802.1p which define CoS for different IP packets. RSVP or DiffServ use those CoS to support their operations.

C.4. IP-MPLS/OTN Architecture

Multi-Protocol Label Switching (MPLS) is a tunneling technology used in many service provider networks. An IP core merges the separate control planes of Layer 2 and Layer 3 networks into a single network. This integration eliminates the management burden of coordinating the operation of two distinct networks, permits

routing and automated traffic engineering to occur on the same platform, and reduces the operational cost of the network. Furthermore, an IP core supporting MPLS offers numerous advantages using traffic engineering to maximize the efficient use of bandwidth and reduce congestion.

Fig. C.9 illustrates IP packet contains MPLS header.

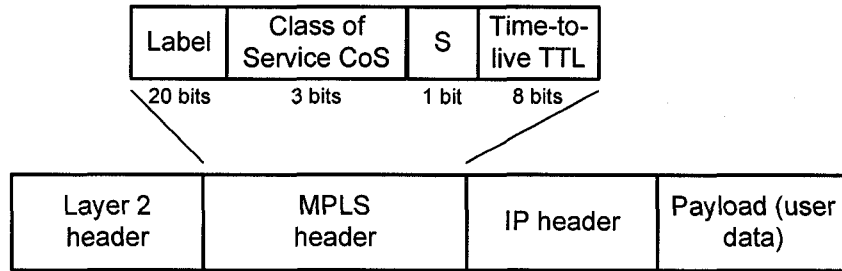


Fig. C.9: An illustration of IP Packet that contains MPLS Header

Each label stack entry contains four fields:

1. A 20-bit label value.
2. A 3-bit field for QoS priority.
3. A 1-bit *bottom of stack* flag. If this is set, it signifies the current label is the last in the stack.
4. An 8-bit TTL (time to live) field.