

Survivability Architectures for Service Independent Access Points to Multiwavelength Optical Wide Area Networks

by

Ananth Nagarajan

B.E. (Electronics), Vivekanand Education Society's Institute of Technology,
University of Bombay, Bombay, India, 1995

Submitted to the Department of Electrical Engineering and Computer Science
and the Faculty of the Graduate School of the University of Kansas in partial
fulfillment of the requirements for the degree of Master of Science

Professor in Charge

Committee Members

Date Thesis Accepted

Shri Ganeshaya Namaha

**This work is dedicated to my beloved parents
R. Nagarajan and Vatsala Nagarajan
who have always blessed and encouraged me in all my endeavors**

Acknowledgements

I thank my advisor and committee chair, Dr Victor Frost, for giving me the opportunity to work on this project and for encouraging and guiding me throughout the course of my study at KU. His timely suggestions and feedback helped me immensely in my work. I would also like to thank Dr Joseph Evans and Dr David Petr for serving on my committee, and Dr Gary Minden for his ideas. Dr Evans' guidance in the project and Dr Petr's excellent teaching have been extremely useful in expanding the horizons of my knowledge in the subject of networking.

I am extremely indebted to my colleagues and friends at KU - Sachin, Shyam, Ranjit, Sampath, Anil, Sandeep, Arvind, Manish, Sudha, Saravanan and many others - with whom I spent many memorable days at KU (and nights at ITTC), had technical discussions and a lot of fun too. They really made life away from home much easier than I thought. My special thanks are reserved for Aarti Iyengar for her care, support and encouragement in everything I did. Thanks are also due to the coffee machine at Nichols, "my" workstation Eckert, Huseyin Sevay's chair that I "inherited" and all the other things that contributed to my research in their own ways.

Last, but surely not the least, I am grateful to my parents - R. Nagarajan and Vatsala Nagarajan - for all their support, encouragement and for giving me the gifts of life and education, my sister - Vidya, for her love and affection, my grandmothers for their care and blessings, all my well-wishers and, above all, to God for giving me the strength and confidence to realize my goals.

Abstract

Recent advances in fiber optics technology have enabled extremely high-speed transport of different forms of data, on multiple wavelengths of an optical fiber, using Dense Wavelength Division Multiplexing (DWDM). It has now become possible to deploy high-speed, multi-service networks using DWDM technology. Many transport network architectures that employ advanced fiber optic technology have been proposed. One such architecture being developed at the University of Kansas is the Service Independent Access Point (SIAP). When multiple services with varying requirements are transported over an Optical Wide-Area Network (O-WAN), it is important to ensure the survivability of each service, and to ensure fast restoration in the event of a failure.

This work addresses the issue of survivability of multi-service networks by developing a generalized framework for evaluating the efficiency of different restoration schemes in terms of the restoration time and the spare capacity requirement. A mathematical representation of the degree of network survivability in terms of the capacity to be restored, link distances and restoration time, is given. In particular, restoration at the WDM, SONET, ATM and IP levels are considered.

The algorithm is applied to an example network topology, and different approaches to restoration are compared. Service-oriented survivability - where the restoration action is performed by the affected service - and Transport-oriented survivability - where the restoration action is performed at the transport layer where the failure originates - are compared. The relative advantages of using a service-independent networking architecture over a traditional layered architecture are also shown. Recommendations based on the result of our comparison are made - these recommendations are generally applicable, although they are derived from the analysis of the example network that is considered in this work.

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Goals for this analysis	3
1.3	Executive Summary	5
1.4	Organization	7
2	The SIAP Architecture - An Overview	9
2.1	Background and Motivation	9
2.2	The Proposed SIAP Architecture	10
2.2.1	Constraints and Assumptions	10
2.2.2	Optical Framing Structure	11
2.2.3	Main Functional Blocks	12
2.2.3.1	Protocols Engine	14
2.2.3.2	Optical Processor	15
2.2.3.3	Link Quality Monitor	16
2.3	Technologies to be developed	19
3	Summary of Service Survivability Schemes for Different Network Layers	21
3.1	Introduction	21
3.2	WDM survivability schemes	22
3.2.1	OA & M for Optical Networks	23

3.3	SONET survivability schemes	25
3.4	ATM survivability schemes	31
3.5	IP survivability schemes	36
3.5.1	ICMP Redirect Message	36
3.5.2	Cisco's Hot Standby Router Protocol (HSRP)	39
3.6	Survivability schemes for different network layers for the SIAP .	41
4	Survivability Approaches and Spare Resource Allocation for the SIAP	44
4.1	Survivability Approaches	45
4.1.1	Service-Oriented Approach	46
4.1.2	Transport-Oriented Approach	49
4.2	Spare Capacity Allocation	51
4.2.1	Layered Spare Capacity Assignment	51
4.2.2	Pre-emptive Spare Capacity Assignment	53
4.3	Summary	55
5	Analysis Methodology, Performance Evaluation of Different Surviv-	
	ability Approaches	56
5.1	Network Survivability Analysis	57
5.1.1	Degree of Survivability	57
5.1.2	Restoration Time	58
5.1.2.1	VWP Protection	60
5.1.2.2	SONET Protection	60
5.1.2.3	ATM Protection (from [8])	61
5.1.2.4	IP Protection	62
5.1.3	Demand Requirements	63
5.1.4	Comments about parameters p and q	67
5.1.5	Algorithm to Evaluate the Performance of Survivability	
	Approaches	68

5.2	A Simple Example to Illustrate the Algorithm	71
5.2.1	Topology	71
5.2.2	Demand Assignment	71
5.2.3	Failure Scenarios	76
5.2.4	Survivability analysis	77
5.2.4.1	Service-Oriented Approach	77
5.2.4.2	Transport Oriented Approach	79
5.2.4.3	Spare Capacity Allocation Schemes	80
5.3	Survivability Analysis of a Practical Network	84
5.3.1	Example Network Topology	84
5.3.2	Demand Assignment	85
5.3.3	Failure Scenarios	89
5.3.4	Survivability Analysis with Service-Oriented Approach	94
5.3.4.1	Failure at WDM level	95
5.3.4.2	Failure at the SONET layer	100
5.3.4.3	Failure at the ATM layer	103
5.3.4.4	Failure at the IP layer	106
5.3.5	Survivability Analysis with Transport-Oriented Approach	106
5.3.5.1	Failure at the WDM Layer	107
5.3.5.2	Failure at the SONET Layer	108
5.3.5.3	Failure at the ATM Layer	109
5.3.5.4	Failure at the IP Layer	109
5.3.6	Spare Capacity Allocation	111
5.3.6.1	Spare Capacity Allocation for Service-Oriented Approach	111
5.3.6.2	Traditional Layered Spare Capacity Allocation for Transport-Oriented Approach	111

5.3.6.3	Pre-emptive Spare Capacity Allocation for Transport-Oriented Approach	113
5.4	Recommendations based on Performance Evaluation of Different Survivability Approaches	115
5.4.1	Service Oriented versus Transport Oriented	116
5.4.2	Service-Transparent versus Layered Network	118
5.4.2.1	Layered Spare Capacity Allocation versus Pre-emptive Spare Capacity Allocation	119
6	Conclusions and Future Work	121
6.1	Conclusions	121
6.2	Future Work	122

List of Tables

3.1	Self Healing Control Schemes - Centralized v/s Distributed[1]	29
3.2	Signal Restoration Level [1]	30
3.3	Rerouting Path Planning [1]	30
3.4	Comparison of SONET survivable architectures [18]	31
5.1	ATM logical layer (4 node network) - demand pattern	73
5.2	ATM logical layer to Physical layer mapping (4 node network)	74
5.3	SONET logical layer to Physical layer mapping (4 node network)	74
5.4	Physical layer working demand requirements (service-transparent network)	75
5.5	SONET layer working demand requirements (layered network)	76
5.6	Physical layer working demand requirements (layered network)	76
5.7	Physical layer spare path assignment	81
5.8	ATM layer spare path assignment	81
5.9	SONET layer spare path assignment	81
5.10	IP logical layer - demand pattern	87
5.11	ATM logical layer - demand pattern	88
5.12	SONET logical layer - demand pattern	88
5.13	Physical Link Working Demands (Transparent Network)	90
5.14	ATM logical Links and native ATM demands and their IP Working Demands (Layered Network)	91

5.15 SONET Links, their native demands and their ATM Working Demands (Layered Network)	92
5.16 Physical Links and their SONET Working Demands (Layered Network)	93
5.17 SONET layer spare capacity assignment	112
5.18 ATM layer spare capacity assignment	112
5.19 IP layer spare capacity assignment	113
5.20 Traditional layered spare capacity assignment	114
5.21 Pre-emptive spare capacity assignment	114
5.22 Comparison of link capacity requirements	115
5.23 Main Findings of our analysis	120

List of Figures

2.1	The SIAP Architecture - Optical Framing Structure (from [26]) . . .	12
2.2	The SIAP Architecture - Main Functional Blocks (from [26]) . . .	13
2.3	Conceptual view of the Link Quality Monitor within an optical terminal (from [9])	17
3.1	Representation of the Optical Network	25
3.2	Protection Switching at the optical layer (from [28])	26
3.3	IP Datagram format for ICMP Redirect message [22]	37
3.4	Example of IP Rerouting using ICMP Redirect message	38
3.5	Illustration of HSRP protocol	39
4.1	Typical multi-layered network with “Client-Server” relationship between network layers	46
4.2	Example network topology	48
4.3	Taxonomy of Network Architectures, Survivability Approaches and Spare Capacity Allocation Schemes	55
5.1	Degree of survivability $s(t)$	58
5.2	Illustration of Dropped and Transit Demand	64
5.3	Flow Diagram for the Algorithm to evaluate different survivability schemes	72
5.4	Simple Example Network - Physical and Logical Topologies . . .	73
5.5	Physical topology of example network	84

5.6	Logical ATM network topology	85
5.7	Logical IP network topology	86
5.8	Virtual Wavelength Path Network	86
5.9	Degree of Survivability as a Function of Restoration Time for SONET protection against WDM layer failures (Service-Oriented Approach, Transparent Network)	96
5.10	Degree of Survivability as a Function of Restoration Time for ATM protection against WDM layer failures (Service-Oriented Approach, Transparent Network)	97
5.11	Degree of Survivability as a Function of Restoration Time for IP protection against WDM layer failures (Service-Oriented Ap- proach, Transparent Network)	97
5.12	Degree of Survivability as a Function of Restoration Time for SONET protection against WDM layer failures (Service-Oriented Approach, Layered Network)	98
5.13	Degree of Survivability as a Function of Restoration Time for ATM protection against WDM layer failures (Service-Oriented Approach, Layered Network)	99
5.14	Degree of Survivability as a Function of Restoration Time for IP protection against WDM layer failures (Service-Oriented Ap- proach, Layered Network)	99
5.15	Degree of Survivability as a Function of Restoration Time for SONET protection against SONET layer failures (Service-Oriented Approach, Transparent Network)	101
5.16	Degree of Survivability as a Function of Restoration Time for SONET protection against SONET layer failures (Service-Oriented Approach, Layered Network)	102

5.17	Degree of Survivability as a Function of Restoration Time for ATM protection against SONET layer failures (Service-Oriented Approach, Layered Network)	102
5.18	Degree of Survivability as a Function of Restoration Time for IP protection against SONET layer failures (Service-Oriented Approach, Layered Network)	103
5.19	Degree of Survivability as a Function of Restoration Time for ATM protection against ATM layer failures (Service-Oriented Approach, Transparent Network)	104
5.20	Degree of Survivability as a Function of Restoration Time for ATM protection against ATM layer failures (Service-Oriented Approach, Layered Network)	105
5.21	Degree of Survivability as a Function of Restoration Time for IP protection against ATM layer failures (Service-Oriented Approach, Layered Network)	105
5.22	Degree of Survivability as a Function of Restoration Time for IP protection against IP layer failures	107
5.23	Degree of Survivability as a Function of Restoration Time for protection against WDM layer failures -Transparent Network, Transport-Oriented Approach	108
5.24	Degree of Survivability as a Function of Restoration Time for protection against WDM layer failures -Layered Network, Transport-Oriented Approach	109
5.25	Degree of Survivability as a Function of Restoration Time for protection against SONET layer failures -Layered Network, Transport-Oriented Approach	110

5.26 Degree of Survivability as a Function of Restoration Time for protection against ATM layer failures -Layered Network, Transport-Oriented Approach	110
5.27 Comparison of Spare Capacity schemes	116

Chapter 1

Introduction

1.1 Motivation

Fiber Optic systems, which support data transport over multiple wavelengths, using Wavelength Division Multiplexing (WDM), have made it possible to realize extremely high bandwidth telecommunication systems. The growth potential of such advanced multiwavelength photonic systems is large, and the capacity is currently constrained only by the termination equipment used. Optical technologies have been employed in the physical layer for some time. Recent advances in WDM technology have enabled multiple wavelengths on a single optical fiber. This, in turn, has enabled the use of WDM in the path layer, and not constrained it to simply physical layer functions. Optical multiplexing and routing techniques are used to reduce electronic processing bottlenecks and to allow a more efficient use of the bandwidth potential of the installed fiber infrastructure. WDM also provides add-drop capabilities wherein only that portion of the total line capacity that needs to be dropped at a node can be terminated, as opposed to termination of the entire line capacity while using Time Division Multiplex (TDM) systems. The total throughput of the optical path cross-connect system can be much larger than that of an electrical TDM

cross-connect system and the hardware can be simplified. Also, each wavelength can be logically viewed as a separate network [3], so various data formats can be transmitted over the same physical facilities. Since WDM offers the ability to multiplex several low-data rate channels, the transmission problems associated with high-data rate systems (like OC-192) may not occur.

The above advantages of WDM systems encourages their use in Optical Wide Area Networks (O-WANs). The transport capabilities of such a network would enable the transport of large amounts of data, in varying formats (like Internet Protocol (IP) datagrams, Asynchronous Transfer Mode (ATM) cells, Synchronous Optical Network (SONET) frames and others) directly on different wavelengths between different nodes of the network. WDM systems thus allow the use of both traditional layered architectures (using different protocols over a standard framing structure like SONET), as well as transparent transport of different services without the intermediate layering. This feature of multi-wavelength systems, as well as the add-drop capabilities provided, motivates the development of service-independent access at the network nodes.

As part of ongoing research in the Lightwave Communications Laboratory, at the Information and Telecommunication Technology Center (ITTC), University of Kansas (KU), work is being done on developing and deploying high speed, Service Independent Access Points (SIAPs)[26] to high capacity O-WANs. Since large amounts of data will be transported via fewer network elements in such a backbone network, many more customers may be affected by single failures, like a fiber-cable cut or any other network equipment breakdown. Fault tolerance and self-healing capabilities are, therefore, imperative in order to ensure the overall survivability of the network. Consequently, it becomes necessary to provide a network infrastructure that is robust to failures and malfunctions of Network Elements (NEs), and is inherently self-healing to allow quick failure recovery.

Many efficient failure recovery schemes[1, 3, 8, 12, 5] have been developed to ensure the survivability of different services like IP, ATM, SONET and even WDM. In future multiprotocol systems, such as the SIAP, it is obvious that there is no single failure recovery scheme that is the best solution for fault-tolerance, because of the interdependence of the different network layers, wherein a single failure at one layer may lead to multiple failures at other layers. This calls for a survivability architecture where different network restoration schemes are activated for different kinds of failure scenarios. Another issue in the design of survivable networks, is the necessity to provide spare capacities (redundancies) for quick restoration. This increases the overall cost of the system. Also, for a multi-service network like the SIAP, spare capacities need to be allocated for each type of service supported. In addition, services must be restored as quickly as possible after a failure. It is clear, therefore, that there are tradeoffs involved in assuring the overall resilience of different services against a set of most frequently occurring failure types, with respect to

1. Initial investment
2. Spare Capacity requirements
3. Restoration times

1.2 Goals for this analysis

This research aims at addressing the above issues by evaluating the performance of different survivability architectures using different service restoration schemes, for different network topologies, sizes and with varying degrees of transparency (i.e., strictly layered architecture, strictly open architecture and a mixture of the previous two architectures). The performance evaluation is done based on the network cost, spare capacity requirements and restoration

speeds of the different survivability schemes. Existing fault recovery methods for different services are used and different approaches that use one or more of the recovery methods, for a given failure scenario, are compared. For this research, we limit the analysis to consider only IP, ATM, SONET and WDM restoration schemes.

In particular, we discuss the following two survivability approaches:

1. The highest-layer survivability approach, where the service that is affected by a failure, performs the failure restoration function irrespective of the actual origin of the failure. We call this approach the **Service-Oriented** approach.
2. The lowest-layer survivability approach, wherein the restoration function is performed by the lowest network layer where the failure originates. The higher layers services are automatically restored by restoring the underlying transport layer. We call this approach the **Transport-Oriented** approach.

We also compare two spare capacity allocation schemes for the above approaches. In the first (traditional) scheme, each network layer or service is assigned its own specific spare capacity. In the second approach, proposed by the University of Ghent [15], a common pool of spare resources is maintained. This spare capacity is shared across network layers using a pre-emptive priority scheme.

Based on the results of the above evaluation, recommendations are made as to which survivability scheme (or group of schemes) is most suitable for a given failure scenario, a given network topology and degree of transparency for the SIAP architecture.

It should be noted that this work is only a preliminary step towards solving the problem of an integrated survivability architecture for multi-service net-

works. Simplifying assumptions about the network architecture, and the ability to map different services on to wavelength paths are made. Nevertheless, this is a first step and a more refined approach towards solving the problem needs to be done in the future.

1.3 Executive Summary

The motivation behind this research is to study the impact of various well-known survivability architectures on future, high-speed multiwavelength optical networks. There exist different efficient survivability schemes for restoring the different network services. In a multi-service network, it becomes important to decide which one (or what combination) of the well-known schemes are best suited for the network, in terms of the network cost and the speed of restoration. With the service transparency and high speed offered by future optical Wide Area Networks, it is interesting to note how the network resilience can be increased, in order to avoid loss of revenue due to failed services.

The main contributions of this research are:

- Developed a generalized algorithm to evaluate different survivability architectures for multi-service networks.
- Evaluated well known schemes for restoration at the WDM, SONET, ATM and IP layers based on their restoration speeds and spare resource requirements.
- Developed recommendations regarding which survivability architecture is most suitable for what kind of a network architecture.
- Showed the advantage of service independent access to multiwavelength OWANs and recommended its use in future high speed networks.

- Explored the relatively new fields of IP restoration and Virtual Wavelength Path Restoration and gave more insight into the different possibilities to restore IP traffic.
- Discussed a novel spare capacity allocation scheme, the pre-emptive scheme [15], showed the cost savings that are achieved using this scheme and showed that the complexity involved in using this scheme can be easily resolved in future multiwavelength networks.
- Developed mathematical expressions relating the network survivability to the restoration time, capacity requirement and link distances for well-known survivability schemes.

The main lessons learned in this research are :

- A service-oriented approach to restoration, where the services affected by a failure perform the restoration action, is seen to be inefficient when a lower-layer failure occurs, because multiple services need to be restored. This approach is, however, suitable for higher layer failures (failures at the service layer itself) and for a service-transparent network. On the other hand, a transport-oriented approach is efficient in terms of the number of restoration actions required, single lower layer failures lead to multiple higher layer failures.
- There is no single best survivability architecture for future multi-service networks. There needs to be a peaceful co-existence of different architectures, that are used in different situations. For example, fast ATM restoration schemes are available, and these can be used whenever possible, irrespective of where the failure occurs. On the other hand, IP restoration is slow and must be avoided unless there is no other way out (like in the case of IP layer failure).

- The importance of planning the network resources, topologies and spare resources in advance in order to quickly restore services from failures is understood. Highly efficient spare capacity assignment techniques, like the pre-emptive approach that is described, should be incorporated in future optical networks. Multiwavelength networks provide the ideal platform for introducing the pre-emptive spare capacity scheme, because spare capacity can be expressed in terms of wavelength paths, irrespective of the type of service being protected.
- The advantage of service-transparent networks over traditional layered networks, in terms of reduced capacity requirements and overhead is an important lesson learned from this research. Service transparency can be achieved easily in multiwavelength networks, by treating each interconnection of Wavelength Paths carrying different services as a separate “logical” network. This motivates research on techniques to achieve service-transparency in future multi-service networks.

1.4 Organization

This thesis is organized as follows.

Chapter 2 describes the proposed SIAP architecture in brief. The main ideas and major components of the SIAP system are presented. An overview of the proposed Operations, Administration and Maintenance (OA & M) features of the SIAP are also discussed. Chapter 3 summarizes different service survivability schemes recommended for different network layers - specifically for WDM, SONET, ATM and IP layers. We also select, for the SIAP architecture, one most popular scheme for each of the four layers, based on factors like recovery time, cost and spare capacity requirement. We define the performance metrics for evaluating the survivability architectures. Chapter 4 describes the two different

survivability approaches - the **Service-Oriented** and the **Transport-Oriented** approaches. In addition, the two spare capacity allocation schemes are discussed. Next, a detailed analytical study of the survivability and spare-capacity approaches for different network topologies, sizes, loads and degrees of transparency is conducted in Chapter 5. These studies are based on known specifications and results of the different survivability schemes[1, 3, 8, 24, 25, 2, 12]. The analysis involves a performance evaluation of each scheme based on the network cost, the spare resource requirements and restoration times. Chapter 6 presents the recommendations based on the results of Chapter 5, the conclusions derived from the work and describes extensions needed to effectively utilize these recommendations for the SIAP.

Chapter 2

The SIAP Architecture - An Overview

2.1 Background and Motivation

The growing demand for bandwidth arises from the increasing dependence on rapid and reliable transport of high quality visual, audio and data traffic for almost every aspect of human interplay - from business, to entertainment, to government, to academia. It is, therefore, necessary to develop technologies for future, extremely high-speed networks and to provide flexible, reliable, high-speed transport for large traffic volumes of different types and with varying requirements.

With the recent advances in lightwave technology, Dense Wavelength Division Multiplexing (DWDM) systems have become a reality. DWDM [20] is a technology that allows multiple information streams to be transmitted simultaneously over a single fiber at data rates as high as the fiber plant will allow. DWDM is ready made for long-distance telecommunications operators that use either point-to-point or ring topologies. The availability of several new transmission channels where there used to be one dramatically improves an oper-

ator's ability to expand capacity and simultaneously set aside backup bandwidth for restoration without installing new fiber (of course, protection against a fiber cut can only be provided with a separate protection fiber). The transparency of DWDM systems to various bit rates and protocols will also allow carriers to tailor and segregate services to various customers along the same transmission routes. Thus, multiple services like IP, ATM, SONET and future new services can be provided on a the same physical transmission route.

We can, therefore, utilize the above features of DWDM systems and to develop Service Independent Access Points (SIAPs) with extremely high speed (hundreds of gigabits per second) switching capabilities, to support multi-protocol switching for optical wide area networks. SIAP is one potential technology for future optical networks. It should be noted that the results of this research are generally applicable.

2.2 The Proposed SIAP Architecture

The SIAP concept is presented in [26], in which it is proposed to design, implement and deploy systems that provide service independent access directly to multiwavelength Optical Wide Area Networks (OWANs).

2.2.1 Constraints and Assumptions

Physical layer attributes and currently available components pose constraints on optical networking systems technologies. Some of these constraints are listed below:

- It is relatively difficult to support large address spaces in all-optical systems due to the cost and complexity of components.
- The frame switching and wavelength re-orientation rates that can be ob-

tained are relatively slow as compared to the gross throughput.

- Sophisticated optical logic devices are unavailable, or, if available, they are extremely expensive.

Due to the above constraints, the SIAP architecture is modeled on the following assumptions:

- The address space used is small because optical correlation is expensive.
- We opt for large frame sizes because optical TDM systems have relatively long matching times and WDM systems have long tuning times.
- Although significant portions of the data path must be optical because of the speed advantage of optics over electronics, portions of the control path may be electronic in order of the relative unavailability of optical logic devices.

2.2.2 Optical Framing Structure

The optical framing structure is shown in Figure 2.1. The features of this structure are :

- Simple headers and trailers
- Fixed frame length (in time)*, to support high speed transmission
- Transparency to higher layer framing schemes (including SONET, ATM, IP and others)
- Rate-independent processing.

The optical frame headers consist of fields to identify the beginning of a frame (preamble), simple addressing based on Virtual Wavelength Paths, some

*The frame length is fixed at 125 μ s, following the SONET frame size

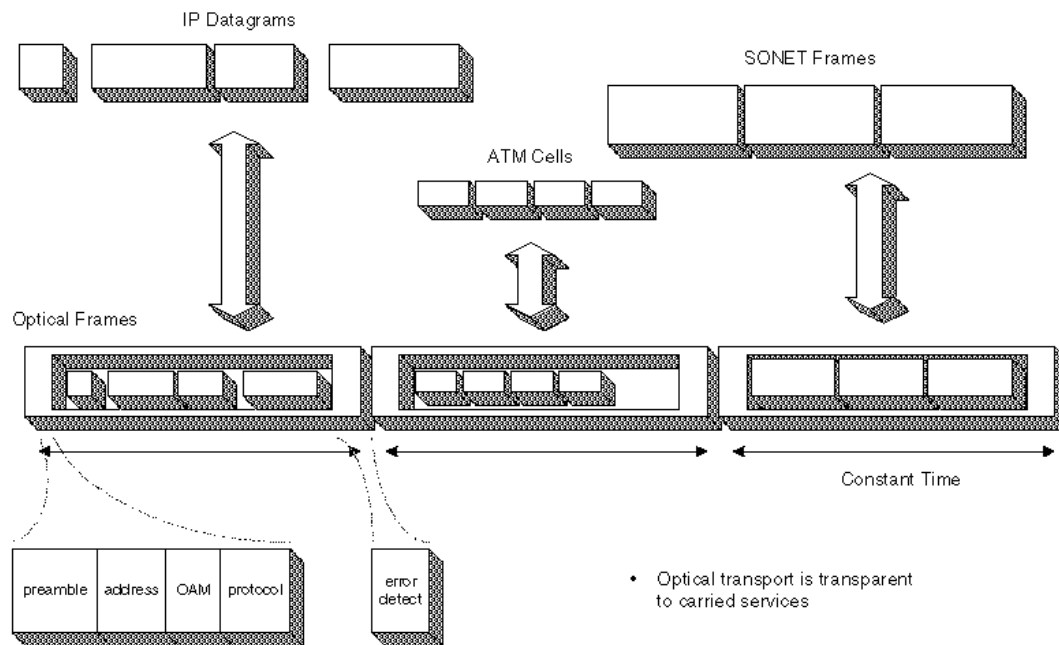


Figure 2.1: The SIAP Architecture - Optical Framing Structure (from [26])

Operation, Administration and Maintenance (OA & M) information, a protocol identifier filed to identify the service protocol encapsulated within the frame and some simple error detecting capability. The above functions are handled by the Optical Processor module of the SIAP architecture, to be described in a later section.

2.2.3 Main Functional Blocks

The main functional blocks of a SIAP node are shown in Figure 2.2. The elements of a SIAP node are:

- A *Protocols Engine* used to convert between existing network services and the O-WAN transmission protocol.
- An *Optical Processor* used to encode transmission frames and select and decode the received frames using high capacity (10 Gbps) optical pro-

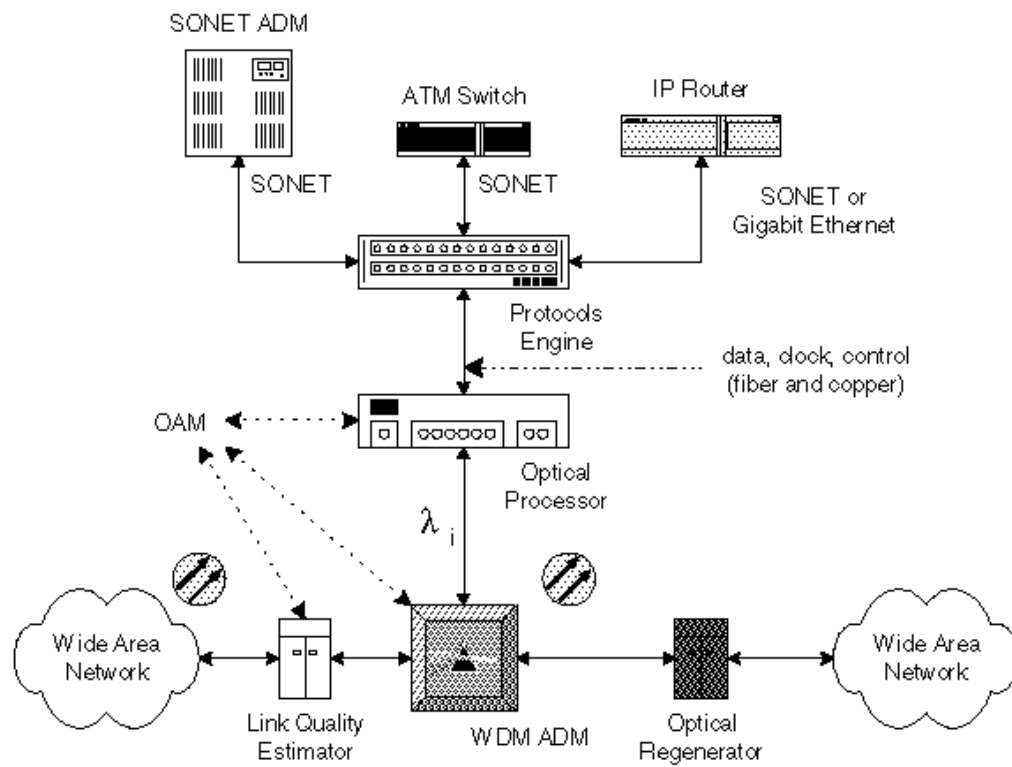


Figure 2.2: The SIAP Architecture - Main Functional Blocks (from [26])

cessing.

- A *Link Quality Monitor* used to estimate signal quality on each wavelength of the WDM system.

In addition, we need elements for the O-WAN system (not specific to the SIAP). These include :

- An *Optical Regenerator* for extracting the timing information from the received signal and regenerating the timing information and amplifying the optical signal. These would be inserted approximately every 3-4 optical segments.
- *WDM Add/Drop Multiplexers (WADMs)* for selecting a single wavelength for further processing from a received WDM signal and injecting a new wavelength into a transmitted signal.
- Protocol-specific engines to transmit and receive different protocols like SONET, ATM, IP or other networking service protocols.

We describe each of the SIAP node elements in some detail below, since these are to be designed according to the SIAP requirements. The other elements, that are general to O-WAN systems are not described, since commercially available equipment will be used.

2.2.3.1 Protocols Engine

The Protocols Engine provides transparent support for multiple higher layer protocols at the bit transport layer. This architecture provides for high performance and flexibility. Bit sequences within the optical framing structure are used to identify the particular service protocol engine (for example, IP router, ATM switch, SONET Add/Drop Multiplexer etc.) to use. Thus, high speeds are supported because unnecessary processing and queuing delays are avoided by

means of direct demultiplexing to upper layer protocol engines. Consequently, this also leads to simplified implementation.

When the Protocols Engine is receiving optical frames, it uses the protocol type identified by a label within the received frame to direct the data to the appropriate protocol-specific engine for processing. For example, if the protocol type indicates that the optical frame consists of ATM cells, then all the data within the optical frame is sent to an ATM switch for processing. It is further assumed here, that each optical frame consists of data of only one type, i.e., each optical frame can contain ATM cells only, or IP datagrams only or some other specific type of service only, but not a mixture of multiple services. Multiple physical layer interfaces, like SONET, Fiber Channel, a clock/data interface etc. may be provided.

On transmission, the Protocols Engine uses control information from the management entity to multiplex streams from the protocol-specific engines. The address/ protocol identifier processing provides the mechanisms for mapping higher layer services to wavelengths and times.

2.2.3.2 Optical Processor

The Optical Processor module is used for encapsulating a flow within a frame and processing the associated framing fields. Datapath, control and management functions are supported by the Optical Processor. These functions include framing, address/protocol identification, scrambling and descrambling and error control. These functions are necessary for the transparent and reliable transmission of arbitrary data sources over the O-WAN.

The framing is done by encapsulating different data formats within an optical frame with a suitable header, as shown in Figure 2.1. Address and protocol identification is done using the appropriate fields in the optical frame overhead. This function is used to identify whether the particular frame is destined

for the present node and to identify the particular service protocol that is encapsulated. Information generated by the management entity is inserted in the transmitted frame and identified on the receive side, to make simple demultiplexing decisions.

Optical clock recovery is one of the most important functions of the Optical Processor module. A signal on a single wavelength is accepted and data and clock signals are recovered for subsequent operations. Work is being done in the Lightwave Communications Laboratory, University of Kansas, on developing an all-optical clock recovery scheme.

Scrambling and descrambling functions will be implemented to provide service independence. A self-synchronous scrambler-descrambler pair based on a standard, simple polynomial (for example, the $x^{43} + 1$ scrambler used for ATM, which requires only delay and a single logical operation) will be implemented.

Relatively weak error detection capabilities will be provided at the optical framing layer in order to minimize processing. Higher layer error handling functions will be used. The alarm indications from the Link Quality Monitor module will also be used to take necessary actions to ensure reliable service and fault-tolerance. Error detection capability of specific fields will be provided through duplication of the address field from header to trailer, to protect these most crucial and critical fields.

The Optical Processor module will require both optical and electronic components.

2.2.3.3 Link Quality Monitor

The Link Quality Monitor (LQM) module is dedicated to monitoring the optical link quality at the optical layer and provides the capability to continuously monitor the condition of the optical fiber communications link to facili-

tate Operation, Administration and Maintenance (OA & M) functions. The implementation details and features of the LQM are described in [9]. The optical link quality is determined by measuring the carrier wavelength, signal power, signal-to-noise ratio and channel modulation. The LQM also facilitates optical layer diagnostics in the event of a channel failure.

The LQM concept is illustrated in Figure 2.3. A sample of the incoming Dense WDM (DWDM) signal with N wavelength channels is routed to the LQM unit and to a demultiplexer, where the signals are separated on the basis of wavelength followed by a bank of typical optical receivers. The LQM analyzes the quality of each channel simultaneously (or very nearly so) and reports to the Optical Processor the status of each channel on a pass/fail basis.

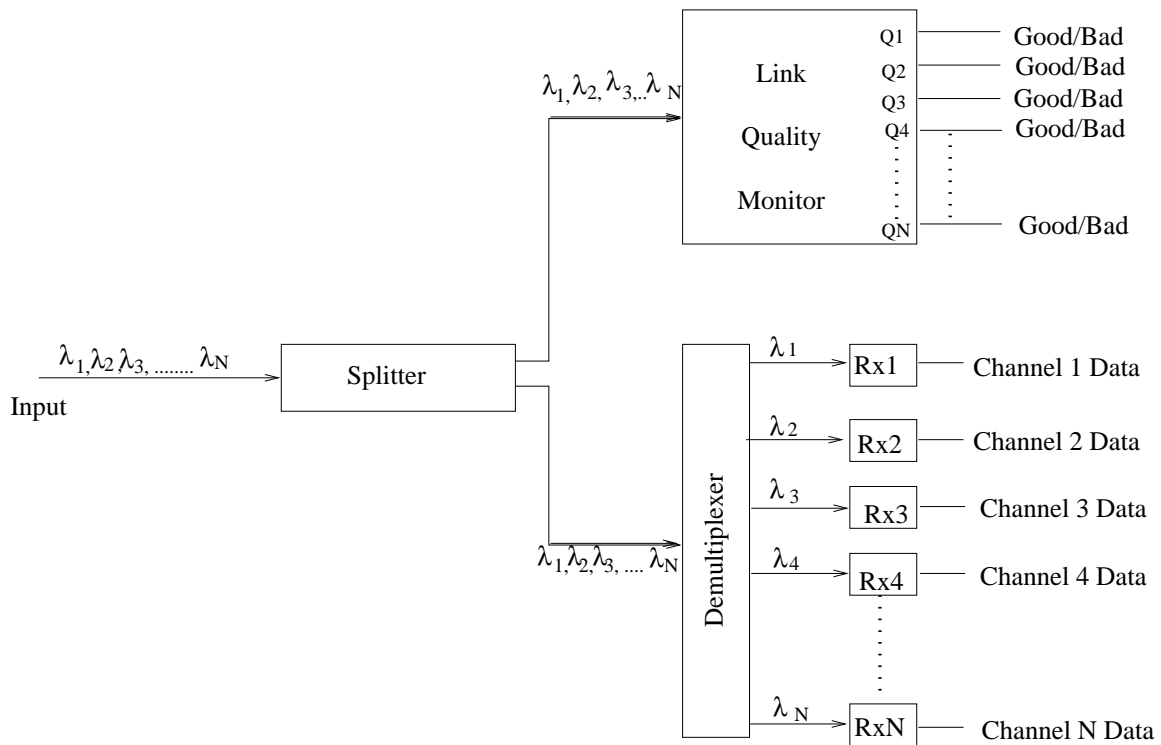


Figure 2.3: Conceptual view of the Link Quality Monitor within an optical terminal (from [9])

The ultimate signal quality metric, i.e., bit-error rate, cannot be readily measured at the optical layer as it requires *a priori* knowledge of the transmitted

signal and conversion into digital data. More fundamental signal parameters that affect the service quality are, therefore, considered for measurement. These include crosstalk, signal wavelength, signal power, signal-to-noise ratio, chromatic and polarization-dependent dispersion and signal modulation. The LQM does not set up the link initially, but monitors changes in the signal quality from a known good state and raises warning flags when these signal parameters exceed acceptable limits. Therefore, certain signal parameters that do not change significantly in a static system configuration, are not considered for measurement in the LQM. These parameters include chromatic dispersion and factors resulting in crosstalk between wavelength channels, like cross-phase modulation, four-wave mixing, Raman scattering etc.

The parameters monitored by the LQM and the information revealed by them are listed below:

- Channel Wavelength monitoring reveals frequency drift in the laser diode (or any wavelength translation devices in the network).
- Channel Power monitoring reveals problems with the laser diode, the Erbium Doped Fiber Amplifiers (EDFAs), or the fiber itself.
- The signal-to-noise ratio measurement will yield insight into the background noise level relative to the signal.
- Monitoring the sideband structure of the spectrum will monitor the health of the modulator and its signaling rate.

Thus, the above metrics enable the supervisory system to isolate the cause of a problem to a particular component, or at least to a small number of components.

2.3 Technologies to be developed

In addition to implementing traditional aspects of a high capacity networking system, the following technologies need to be developed in order to implement the SIAP architecture:

- A new optical framing structure based on the goals of rate independence and constant time, as shown in Figure 2.1, needs to be developed. The Optical Processor will be able to process the received signal and pass it to the Protocols Engine. A constant time frame structure (for example, 125 μs like SONET) allows scaling to higher data rates in the future.
- Capacity allocation strategies must be implemented to respond to customer demands from time to time. Capacity allocation needs to be done between two or more SIAPs.
- The LQM capability is a prerequisite for OA & M support. A single management entity is required to monitor multiple wavelengths efficiently. OA & M information is extracted using the LQM and the required action is taken using separate OA & M channel wavelength (the supervisory channel).
- The optical layer must provide protection against problematic bit sequences that might introduce clock tracking errors. Robust timing provisions need to be made by using a sophisticated clock recovery mechanism and bit sequence independence through all-optical scrambling. A standard self-synchronous scrambler-descrambler pair, that can be implemented relatively simply without complex control mechanisms, needs to be developed for all-optical scrambling. The clock recovery and scrambling functions provide independence of the optical layer from the higher layer protocols.

- Optical regeneration needs to be developed in order to best utilize the SIAP architecture in O-WANs. This is because commercially available WADMs do not support all optical regeneration.

The SIAP concept is an example of a future network technology involving multiple services. In order to realize the potential of this technology, it is necessary to ensure its reliability and fault-tolerance. It is critical to protect the multiple services from network failures. Also, each network service has its own special set of survivability requirements and restoration schemes. It is necessary to study the survivability architectures for the different network services, in order to find out what it needs to make this future technology fault-tolerant. Only then will new technologies like the SIAP be practically realizable. The survivability architectures for existing network services, that need to be supported in the SIAP, will be studied in the next chapter.

Chapter 3

Summary of Service Survivability Schemes for Different Network Layers

3.1 Introduction

Network integrity has gained prime importance with our increasing dependence on communications technology. A very high level of service availability is becoming imperative, for both the service user and the service provider, in order to minimize huge losses of revenue in case of lost communications services. Since future backbone networks will be composed of multiple technologies, it is important to provide survivable transport to the different services in a multi-layer, multi-service network environment. The SIAP architecture, in particular, allows for the transport of different services like IP, ATM and SONET over a WDM-based network. In a multi-service environment, there are different recovery schemes for the different services. These recovery schemes need to be coordinated in order to improve the overall availability of the network in a cost-effective way.

In this chapter we describe in brief, the most popular survivability schemes at each different network layer and their relative merits. In particular, we discuss approaches for service restoration at the WDM, SONET, ATM and IP layers.

3.2 WDM survivability schemes

Present transport network technologies use optical technologies only at the physical media layer, for point-to-point transmission. Existing path technologies are based on electrical technologies. There are several advantages, however, to the use of optical technologies in the path layer. Optical technologies are especially important for network restoration, which is usually carried out at the path layer [1]. When the optical path is used for restoration, a major portion of the network restoration systems will be used in common by different transfer modes, which results in the realization of more effective network restoration. Optical paths are identified by wavelengths and they accommodate electrical paths.

The Wavelength Path (WP) and the Virtual Wavelength Path (VWP) are the two types of optical paths that have been developed [3, 31, 32]. The VWP scheme is used to allocate wavelengths link-by-link and hence, the wavelength assignment is local to a link as opposed to global i.e., it is not necessary to dedicate the same wavelength in each link for a VWP. WPs use global allocation of wavelengths, i.e., a WP is characterized by the same wavelength on each link. VWPs can be considered similar to the Virtual Paths (VP) of ATM networks. VWPs have the following advantages over WPs:

- Simple path accommodation design
- Greater flexibility in network expansion

- Fewer network resources (wavelengths or fibers) required

The disadvantage of VWPs, however, is that they require wavelength conversion at cross-connect points, which can be expensive. In order to minimize costs, VWP protection strategies using limited wavelength conversion have been proposed in [5]. VWP accommodation design strategies are discussed in [32]. These strategies aim at reducing the number of wavelength conversions required by using different efficient wavelength routing algorithms and logical WP (VWP) network topologies. The design of logical topologies for multiwavelength networks is discussed in [30]. Different schemes for the design of Optical paths using WP and VWP, with and without considering restoration are also discussed in [31], [3] and [32].

3.2.1 OA & M for Optical Networks

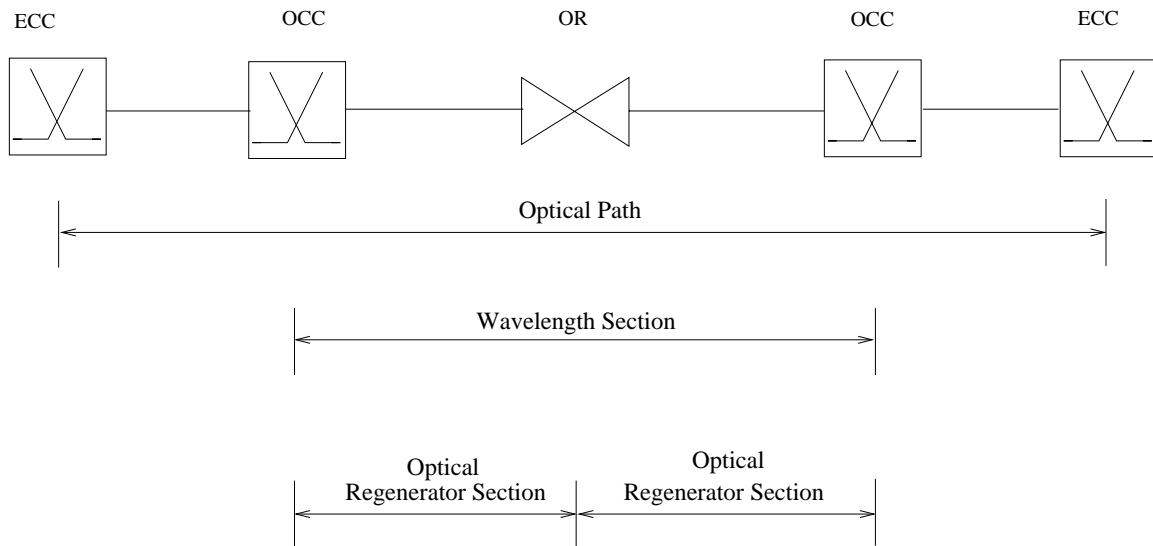
Operations, Administration and Maintenance (OA & M) for the optical network deals with the supervision of optical regenerators, the maintenance signals required for failure localization, and the difficulty of defining a suitable mechanism for performance monitoring in transparent networks. In order to perform the OA & M functions, it is convenient to divide the optical network into a layered model, like the SONET Section, Line and Path.

Since the smallest unit of a multiwavelength optical network is a single wavelength channel, rather than a single fiber, it is necessary to introduce a layer to identify the wavelength. In [27] and [28], a layered model for the optical network is discussed. The generic approach to a layered OA & M model involves a client/server relation between adjacent layers. Each layer is characterized by a specific signal - the characteristic information. The characteristic information of the client layer is transported by the server layer after an adaptation function (involving multiplexing, coding, etc.) is performed on it. This

characteristic information is carried in an Overhead Channel (or OA & M channel) across the network elements. The layers introduced in the optical network are [28]:

- Optical Path layer - where the cross-connecting of virtual wavelength paths occurs.
- Wavelength Section layer - along each wavelength section, the wavelength of the optical carrier is constant, but may vary from section to section. Many wavelength sections constitute an optical path.
- Optical Regenerator Section layer - this layer represents the the most basic part of the optical network, the connection between optical regenerators. In general, a Wavelength Section consists of many Optical Regenerator sections.

The representation of the optical network in terms of the above three layers is shown in Figure 3.1. Each of the above layers transfers maintenance information via its respective Overhead bytes, which form the OA & M channel. Protection switching can be implemented in the optical network, in order to restore failed demands. Protection switching in the optical network can be done at the optical regenerator section, or the wavelength section or the optical path section[28]. Each of these three alternatives is shown in Figure 3.2. For effective protection against fiber damage, the working and protection fibers should be laid on disjoint routes. In the case of the optical regenerator section protection, this does not seem to be practical, as the regenerator section is very small. On the other hand, optical path protection protects the Electrical Cross Connect at the expense of doubling the Optical Cross Connects, as shown in Figure 3.2. The best choice, therefore, turns out to be wavelength section protection which not only deploys redundant fibers, but also redundant optical regenerators. Therefore, it is recommended to use Wavelength Section Protection (using



ECC - Electrical Cross-Connect
 OCC - Optical Cross -Connect
 OR - Optical Regenerator

Figure 3.1: Representation of the Optical Network

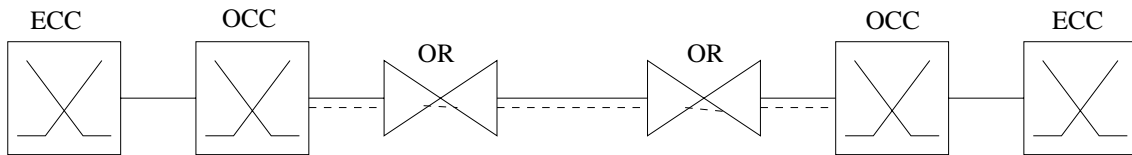
Wavelength Path (WP) or Virtual Wavelength Path (VWP) switching) [3] as the protection scheme at the WDM layer.

3.3 SONET survivability schemes

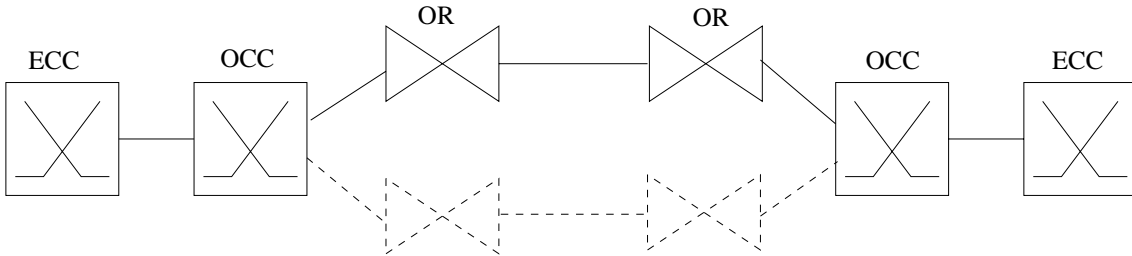
The SONET Frame structure and Hierarchy for the Synchronous Transport Signal- Level 1 (STS-1) are explained in [1, 19]. The SONET Frame consists of two sections : the Transport Overhead and Information Payload. The former consists of the Line Overhead and Section Overhead, whereas the latter has a Path Overhead and a Synchronous Payload Envelope (SPE). An STS-1 SPE can carry one DS3 or more sub-DS3 signals called Virtual Tributaries (VT's). The K1 and K2 bytes in the Section Overhead are used for protection.

SONET has four interface layers - Path, Line, Section and Physical layers. The SONET Overhead Channels are divided into three layers - Section, Line and

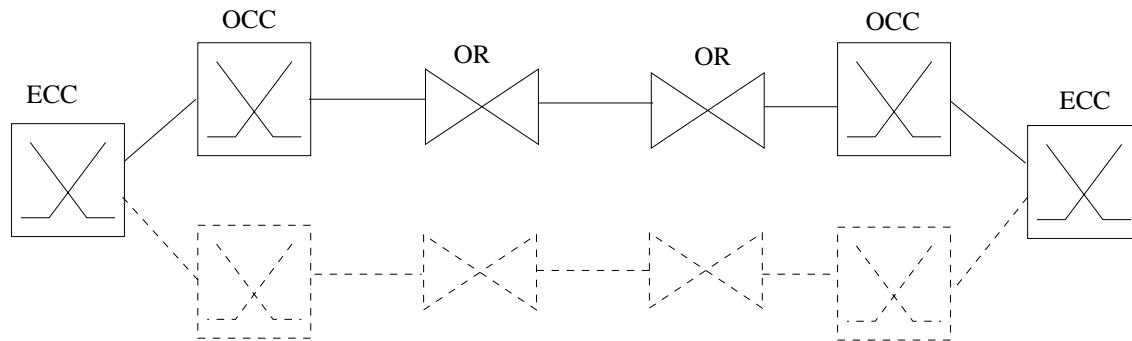
Protection of optical regenerator section



Protection of wavelength section



Protection of optical path



The working entity is shown with solid lines, the protection entity with dashed lines.

ECC - Electrical Cross-Connect OCC- Optical Cross-Connect OR - Optical Regenerator

Figure 3.2: Protection Switching at the optical layer (from [28])

Path. SONET uses the pointer method for multiplexing, which is more flexible, allows the transport overhead to be decoupled from the SPE, allows bit-stuffing to accommodate slight frequency variations, easy access to tributaries and direct access to VT signals without demultiplexing the entire STS-1 Frame because the VT locations are identified by the pointer values.

A Digital Cross-Connect System (DCS) is a network element that terminates digital signals and automatically cross-connects constituent (tributary) signals according to a map stored in an electronically alterable memory. These systems are useful in dynamic restoration because they provide spare capacities. SONET Digital Cross-connect Systems (DCS) are used to terminate SONET signals (like STS-1 and OC-N) and cross-connect them, in addition to terminating and cross-connecting normal digital signals like DS1 and DS3.

One of the initial major benefits that was provided by SONET is network survivability. SONET requires some initiation criteria for protection like Signal Failure (SF) and Signal Degrade (SD). These trigger off alarms like Loss of Signal (LOS), Loss of Frame (LOF), Bit Error Ratio (BER) exceeding 10^{-3} [1], Alarm Indication Signal (AIS). Failure States must be reported to the Operations System (OS). Maintenance Signals are also available to alert the SONET NE's of detection/location of the failure.

Three network protection schemes are commonly defined, based on ITU-T Recommendations G.841 and G.842 [24, 25]. They are :

1. Protection switching

Automatic Protection Switching (APS) and Dual Homing (DH) are the two techniques that fall under Protection Switching.

- **Automatic Protection Switching(APS)**

APS automatically reroutes signals from a working line to a protection line during signal outage. Thus it provides a method to carry service for planned outages, like new equipment installation and

routine maintenance, and also provides a line restoration capability in case of unexpected outages, such as failures. It is the simplest and fastest facility restoration scheme. 1:N APS is a system where there is one protection fiber for N fibers. Thus, it can restore a single-fiber system failure; however, it is not effective for fiber cable cuts because the protection fiber is placed in the working fiber sheath and could also be cut. 1:N Diverse Protection Switching is an economic, although not 100 per cent survivable, alternative for Automatic Protection Switching [1]. In Diverse Protection (DP), the protection fiber is placed away from the working fibers. Thus it can partially restore services from a fiber cable cut. 1:1 protection has a protection fiber for every working fiber, and therefore, is completely survivable. However, it is also costly. APS is achieved in SONET using the K1 and K2 bytes of the Section Overhead in the SONET payload. In Automatic Protection Switching, we also have 1+1 switching, which is a form of 1:N switching with the head end of the fiber system permanently bridged. In order to reduce costs, by eliminating Path Terminating Equipment (PTE's), Optical Protection Switching is suggested in [1].

- Dual Homing

Dual Homing is an office backup concept that assigns two hubs to each office and requires dual access to other offices. In the DH architecture, demand originating from a special office is split between two hubs: a home hub and a designated foreign hub. In the case of a home hub failure, an office that uses dual homing can still access other offices via the backup hub. The different schemes in Dual Homing are considered in [1].

2. **Rerouting** : Rerouting involves the establishment of a replacement connection by the network management control connection.
3. **Self Healing Mesh and Ring Networks** : Two restoration schemes are implemented namely: Line restoration and Path restoration, depending on which layer is being used as the protection layer. The DCS self-healing network is economical in areas where high demand and high connectivity are involved.

Reconfigurable DCS networks are usually used for flexible network control (Bandwidth Management) and restoration (DCS Self Healing network). The former is concerned with frequent, but limited failures and centralized control schemes are often employed. The latter is concerned with catastrophic failures and distributed schemes are preferred.

The restoration sequence employed in DCS Self Healing networks is detection, control message propagation, route selection, rerouting and return to normal. The comparison between Centralized and Distributed Control of Self Healing Networks is shown in Table 3.1.

Table 3.1: Self Healing Control Schemes - Centralized v/s Distributed[1]

Feature	Centralized	Distributed
Vendor independence and interoperability	easy	difficult
System complexity	simple	complex
Demand restoration probability	higher	lower
Return-to-normal	easy	difficult
Standards needed	messages only	algorithm and messages
Coordination between capacity planning and real time restoration	easy	difficult
Restoration time	slower (minutes)	faster (seconds)
System vulnerability	higher	lower
Administration overhead	higher	lower

The comparison between Line Restoration and Path restoration for Self Healing Networks is shown in Table 3.2. The comparison between pre-planned and

Table 3.2: Signal Restoration Level [1]

Feature	Line Restoration	Path Restoration
Restoration speed	faster	slower
Rerouting decision complexity	simple	complex
Efficient use of spare capacity	worse	better

dynamic re-routing is shown in Table 3.3.

Table 3.3: Rerouting Path Planning [1]

Feature	Preplanned Rerouting	Dynamic Rerouting
System complexity	lower	higher
Network adaptation	difficult	easy
Restoration speed	faster	slower
System Reliability	lower	higher
Memory requirement	higher	lower

SONET Self Healing Rings (SHR's) use add-drop multiplexers (ADM's), and use 1:1 protection switching while also providing for fiber capacity sharing. Thus they provide more survivability while reducing cost. SONET SHR's are of two types : Unidirectional (USHR) and Bidirectional (BSHR). BSHRs can have either 4 fibers (2 working and 2 protection fibers) or just one fiber wherein half of the fiber system bandwidth is reserved for protection. The above two schemes are BSHR/4 and BSHR/2 respectively. BSHR/4 can use WDM to reduce the number of fibers to 2 instead of 4. A detailed analysis of each of these architectures is given in [1].

Another SHR architecture that uses WDM is SHR/WDM which requires optical components. It is easier and less expensive to upgrade and the ring size is limited only by the number of wavelengths available and not by electronics. Also Electrical to Optical Conversion (E/O) is not required if optical amplifiers are used. It has a shorter average transport delay.

The different SONET survivable architectures are compared in Table 3.4. It

Table 3.4: Comparison of SONET survivable architectures [18]

Attributes	APS/DP	SHR/ADM	DCS Mesh
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	Seconds/minutes
Software Complexity	Least	Moderate	Most
Protection against major failure	Worst	Medium	Best
Planning/Operations Complexity	least	Moderate	Most

is seen from the above discussion, that SONET SHR/ADM is the most suitable survivability architecture for SONET. Large networks can be formed by inter-connecting SONET SHRs. It should also be noted that although pre-planned restoration path planning is not efficient, it is often advisable to plan the restoration paths in advance in order to avoid the dynamic path computation time. It is recommended to use SONET SHRs wherever possible, or else use 1:1/DP whenever the network topology is not a ring. When restoration speed is very critical, it is recommended to use pre-planned restoration path assignment, along with line switching.

3.4 ATM survivability schemes

ATM networks have some intrinsic features for fast restoration [8]. They are:

- ATM cell-level error detection, in the form of a header error check (HEC) sequence, increases the overall error check sampling rate per transmission interface and thus provides a means for enhanced failure detection and alarm threshold protocols. Since the cell is a small unit, a large number

of HEC checks are available per unit time and, therefore, discrimination between different error rates can be performed with high confidence in small intervals of time. On the contrary, the SONET frame duration is 125 microseconds, irrespective of transmission speed. Therefore, fewer checks are available per unit time in the case of SONET. Besides, the parity check present in the SONET frame overhead covers a large number of bits and therefore, its error discrimination capability is poorer.

- Inherent rate adaptation and non-hierarchical multiplexing allow for flexible interface structures and elimination of multiplexing stages within the network. This allows for increased link capacity utilization, flexible interface structures and elimination of multiplexing stages within the network, which results in flexible link network reconfiguration and dynamic bandwidth control. These factors can be combined to yield faster network reconfiguration methods for ATM with lower spare capacity requirements as compared to STM. It has been shown in [8] that failure detection in ATM-based networks is much better than STM-based networks.

A very good feature of ATM networks is that a VP route can be established without assigning its bandwidth along the path. An optimal VP routing for survivable ATM networks is found in [7]. Survivable ATM network management requires complicated procedures since resource allocation requests from ATM cells, calls and virtual paths have to be handled effectively to meet the specified Quality of Service(QoS). A layered switching architecture [8, 7, 17] is proposed to reduce this complexity. The network management process is simplified by classifying different types of network resources and traffic entities into layers. These layers and their functions are:

1. Facility network layer : This is the highest layer. Facility network planning is done in this layer. Survivability QoS is also taken care of partially.

2. Virtual Path layer: The VP manager configures virtual paths so that the survivability measure is optimally enhanced. It also performs fast VP restoration when a failure occurs. If the VP manager is unable to maintain the desired survivability measure at a desired level due to a growth of traffic demand, the facility network layer must initiate a facility network process. Path level recovery enables a rapid and efficient restoration and considerably reduces the complexity of traffic management.
3. Call layer: This gives the call-level QoS to the VP layer. It does admission control and dynamic call routing.
4. Cell layer : It submits the cell-level QoS to the Call manager. It takes care of Traffic enforcement, smoothing and priority buffering.

The ATM switched network alternatives [1] are:

- ATM VC-based switched network (or simply ATM switch). It is associated with call processing and path bandwidth management.
- ATM VP-based switched network (or ATM/DCS). It does not have call processing, bandwidth and routing functions, but simply transports signals transparently.
- Hybrid ATM/SONET switched network. This is discussed in [1].

Whenever a failure occurs, it is possible to reroute the affected traffic using the available spare capacity. Various algorithms that search for spare capacity in the network are discussed in [1]. The dynamic capacity search process, however, is slow, and may not yield 100 % restoration. Therefore, it is better to plan for fastest possible restoration using the frequently occurring failure conditions, by providing sufficient redundant capacity. This argument is similar to the one made in the case of SONET protection, where we stated that pre-planned restoration paths lead to faster restoration.

The restoration algorithms have an effect on the restoration speed of the VP's, processing and memory requirements on the nodes and the redundant capacity needed. The different algorithms considered in [8] are :

1. Local Rerouting:

All VP's on a failed link are rerouted locally around the failed link. It is simple but it is possible that all the VP's are processed by the same set of nodes, hence, leading to a bottleneck. Besides, unnecessary assignment of redundant capacity can take place.

2. Source-based Rerouting:

Each VP affected by a link failure is processed and rerouted individually. Thus, it reduces hop-count by looking at choices for rerouting, and selects a path with minimum redundant capacity requirements. However, memory burden on the nodes is larger and restoration time may be longer.

3. Local Destination Rerouting:

It is a combination of the above two methods. The VP's are allowed to compute the best alternate route. Back-hauling is avoided.

Different survivable architectures using ATM are discussed in [1]. These are the ATM-VP based architectures like ATM/DCS/SHR and ATM/DCS Self Healing Mesh. The design of ATM/DCS/SHR requires the following modules:

- ATM-SONET interface.
- Header processing.
- Service Mapping.

Restoration using VP Self-healing capabilities are seen using both centralized and distributed control [3, 8]. A hybrid approach combining the above control schemes is suggested[8]. This involves centralized computation of alternate

paths in order to avoid large processing power requirements for nodes. After computing the alternate paths using routing tables, the central processor downloads the appropriate tables to the nodes. Each node only stores the table it needs to activate, thus increasing the speed of restoration. This hybrid approach was tested using a simulation of a failure scenario and is shown to be highly advantageous.

Self-healing using distributed control is discussed in [3] and uses logical realization of VP's. Existing self-healing algorithms require at least one round-trip exchange of restoration messages between sender and chooser nodes (restoration pair nodes). However, in the algorithm described in [3], restoration path establishment is completed with the transmission of restoration message in only one direction.

Finally, a comparative study on restoration schemes of survivable ATM networks is done in [33]. It clarifies the benefits of end-to-end restoration schemes quantitatively through a comparative analysis of the minimum link capacity installation cost.

Based on the above discussion, and the comparison of different ATM restoration schemes described, the most suitable restoration scheme appears to be the fast ATM VP restoration scheme described in [8]. By pre-planned allocation of spare VPs, this scheme yields very high restoration speeds, as will be shown in Chapter 5.

3.5 IP survivability schemes

The Internet Protocol (IP) [21] is used for host-to-host datagram service in a system of interconnected networks. The network connecting devices are called Gateways. These gateways (henceforth called routers*) communicate between themselves for control purposes via a Gateway-to-Gateway Protocol (GGP) [23]. In the event of a route failure between two hosts, we could use conventional re-routing schemes like the Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and the Open Shortest Path First Protocol (OSPF) [21] to establish alternate routes. These schemes would essentially cause the datagram flow to be routed via a different router, in the event of the working connection between two nodes breaking down. However, since the two hosts are statically configured with the address of a single router, the nodes will be able to communicate again only if the configuration of the hosts is dynamically changed to reflect the new router. Because of such inherent limitations of the conventional re-routing protocols, they are not discussed here.

We shall discuss two possible sets of failures in the transport of IP datagrams. In the first case, we consider the inability of the network to deliver datagrams from the source host to the destination host due to failure in the existing (or default) route. In the second case, we discuss a strategy for handling router failures.

3.5.1 ICMP Redirect Message

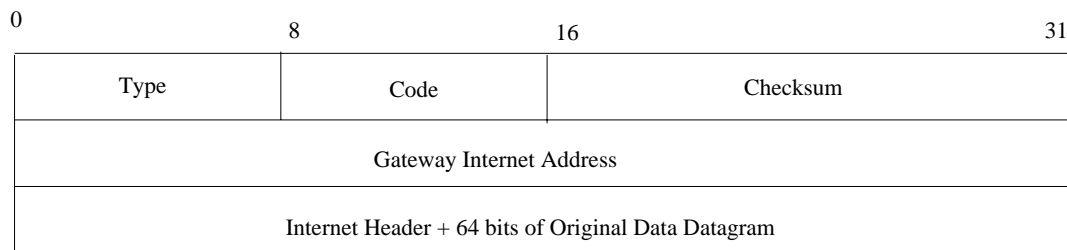
IP is not designed to be absolutely reliable. In order to provide feedback about problems in the communication environment between the destination host and

*The technical meaning of a gateway is a hardware or software configuration that translates between two dissimilar protocols. A router, on the other hand, is a special-purpose computer (or software package) that handles the connection between 2 or more networks. For the purpose of this discussion, the two terms can be used interchangeably

the source host, the Internet Control Message Protocol (ICMP) [22] is used. ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the router does not have the buffering capacity to forward a datagram, and when the router can direct the host to send traffic on a shorter route.

The ICMP redirect message format is shown in Figure 3.3. An ICMP Redi-



Type = 5

Code

0 = Redirect datagrams for the Network

1 = Redirect datagrams for the Host

2 = Redirect datagrams for the Type of Service and Network

3 = Redirect datagrams for the Type of Service and Host

Checksum = 16-bit ones' complement of the ones' complement sum of the ICMP message starting with the ICMP Type

Gateway Internet Address = Address of the gateway to which traffic for the network specified in the internet destination network field of the original datagram's data should be sent

Internet header + 64 bits of Data Datagram = Data used by host to match the message to the appropriate process.

Figure 3.3: IP Datagram format for ICMP Redirect message [22]

rect tells the recipient system to over-ride something in its routing table. It is legitimately used by routers to tell hosts that the host is using a non-optimal or defunct route to a particular destination, i.e., the host is sending it to the wrong router. The wrong router sends the host back an ICMP Redirect packet that tells the host what the correct route should be.

Consider the example network shown in Figure 3.4. The router sends a

redirect message to a host in the following situation. A router, G1, receives an

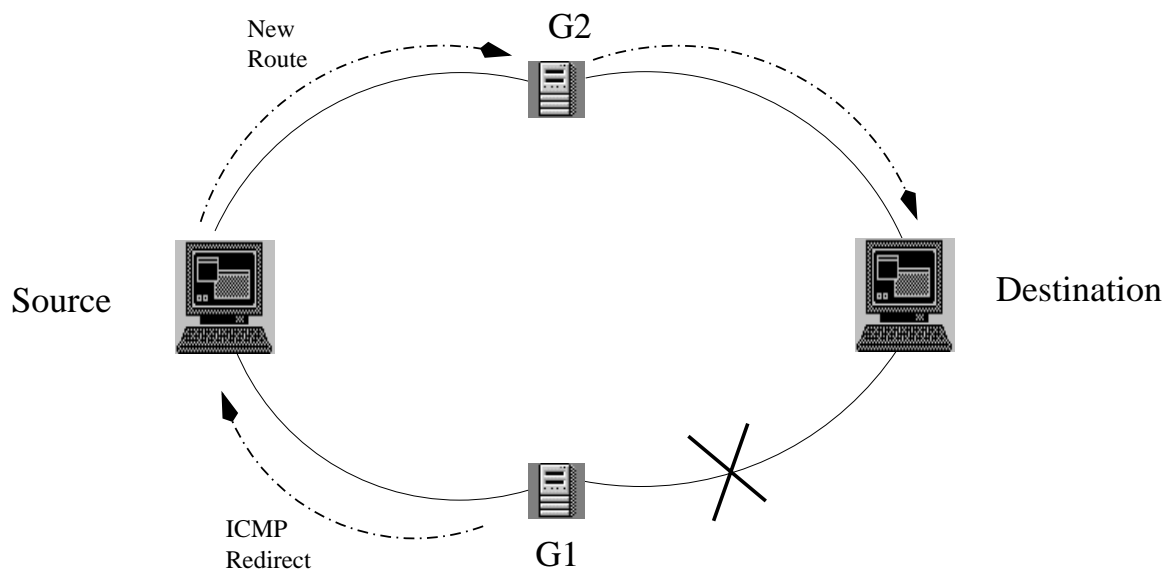


Figure 3.4: Example of IP Rerouting using ICMP Redirect message

internet datagram from a host on a network to which the router is attached. The router, G1, knows that the route to the destination has failed. It, therefore sends an ICMP redirect message to the host, asking it to send the datagram to a different router, G2, on the route to the datagram's internet destination network. The router G2 forwards the original datagram's data to its internet destination.

For datagrams with the IP source route options and the router address in the destination address field, a redirect message is not sent even if there is a better route to the ultimate destination than the next address in the source route. Codes 0, 1, 2, and 3 (shown in Figure 3.3) may be received from the redirecting router based on which datagrams need to be redirected. These codes enable the redirection of datagrams for the network, or datagrams for the Host, or datagrams for the Type of Service and Network or those for the Type of Service and Host.

The disadvantage of ICMP Redirect is that it could pose possible security problems if used maliciously. For example, the routing tables on the host can

be altered to possibly subvert the security of the host by causing traffic to flow via a path the network manager didn't intend. ICMP Redirects also may be employed for denial of service attacks, where a host is sent a route that loses it connectivity, or is sent an ICMP Network Unreachable packet telling it that it can no longer access a particular network.

3.5.2 Cisco's Hot Standby Router Protocol (HSRP)

Cisco's Hot Standby Router Protocol [12] is used when datagram delivery fails because of a failed router. Advanced IP routing protocols like Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and Open Shortest Path First (OSPF) [21] respond to network failures very quickly and can usually recompute an alternative route in a matter of seconds. The HSRP helps such routing protocols to fully utilize their fast rerouting capabilities.

To illustrate how HSRP works, let us consider the network in Figure 3.5. Router A handles packets between Node A and Node C, and Router B handles

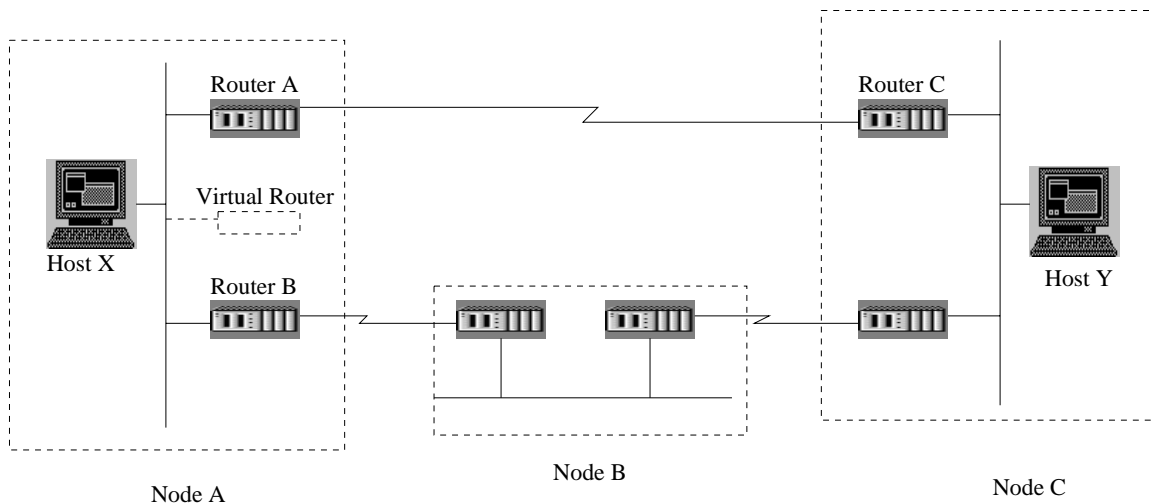


Figure 3.5: Illustration of HSRP protocol

packets between Node A and Node B. If the connection between Routers A and C goes down, or if either router becomes unavailable, conventional re-routing

schemes like Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) and Open Shortest Path First Protocol (OSPF) would prepare Router B to transfer packets that would otherwise have gone through Router A. However, Host X and Host Y would still be unable to communicate with each other, as they are statically configured with the address of a single router, such as Router A. Communication between the IP hosts will be possible only if the configuration of Host X is changed to Router B instead of Router A.

HSRP provides a way to keep communicating without the need to modify the host configurations. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a “virtual” (or “phantom”) router. The virtual router does not physically exist - instead, it represents the common target for routers that are configured to provide backup to each other.

Thus, Host X is configured with the IP address of the virtual router as the default router. Router A is configured as the active router. It is configured with the IP address and MAC address of the virtual router and sends any packets addressed to the virtual router out to Host Y. Router B is also configured with the IP address and MAC address of the virtual router. If, for any reason Router A stops transferring packets, the routing protocol converges, and Router B assumes the duties of Router A and becomes the active router. Router B now responds to the virtual IP address and the virtual MAC address, and Host X can still use the IP address of the virtual router to address packets destined for Host Y, which Router B receives and sends to Node C via Node B.

HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. The active router is assigned a priority that is higher than the priority of all other HSRP-configured routers.

HSRP works by the exchange of multicast “HELLO” messages that advertise priority among HSRP-configured routers. When the active router fails to send a hello message within a configurable period of time, the standby router

with the highest priority becomes the active router. The transition of packet-forwarding functions between routers is completely transparent to all hosts on the network.

HSRP-configured routers exchange three types of multicast messages :

1. Hello - This message conveys to other HSRP routers the router's HSRP priority and state information. By default, the HELLO time is 3 seconds.
2. Coup - A coup message is sent by a standby router when it assumes the function of the active router.
3. Resign - This message is sent by an active route which is about to shut down or when a router that has a higher priority sends a Hello message.

At any time, HSRP-configured routers are in one of the following states:

- Active - The router is performing packet-transfer functions.
- Standby - The routers is prepared to assume packet-transfer functions if the active router fails.
- Speaking and Listening - The router is sending and receiving hello messages.
- Listening - The router is receiving hello messages.

It should be noted that when the HSRP protocol is being used, ICMP redirects cannot be used. Thus the two restoration schemes are mutually exclusive.

3.6 Survivability schemes for different network layers for the SIAP

For the SIAP network, since multiple services are provided, a high degree of network survivability is desirable. We have seen different restoration schemes

for the different network layers. It is important that network restoration is fast, and at the same time, efficient in terms of resources required and low cost. Since 100 % survivability and fast restoration are the objectives, we opt for pre-planned restoration path assignment (where the spare capacity and spare paths are pre-allocated) rather than dynamic re-routing capabilities (where restoration paths are dynamically searched for after a failure event). Although a pre-planned spare capacity allocation and restoration path allocation is not efficient, it guarantees the desired degree of survivability. Time consuming path-search algorithms are avoided.

For our analysis of a future multi-service network, such as the SIAP, we shall consider the following restoration mechanisms, based on the features and advantages of each of the restoration mechanisms discussed in the previous sections:

- For WDM failures, we use the VWP restoration scheme [3], with pre-allocated spare VWPs. Pre-allocation of spare VWPs avoids time-consuming path-search procedures after a failure takes place. The VWP restoration scheme for wavelength section protection is also the most popular restoration scheme at the optical layer[3, 28].
- For recovery from SONET failures, we use the SHR/ADM restoration, since it is very fast, and less expensive than APS/DP. Large networks can be configured to look like several interconnected SHRs. In case a ring topology is not available, 1:1 APS/DP is the restoration scheme that will be used. As in the case of the WDM restoration, restoration paths are pre-assigned.
- For recovery from ATM failure, we use the fast VP restoration scheme described in [8]. As will be seen in the chapters to come, this scheme has a clear restoration speed advantage as compared to the other schemes.

- IP failures are recovered using CISCO's HSRP protocol. This protocol can be efficiently applied to any IP network, and can be used to protect against Router failure, as well as against failed links between two routers. It should be noted that, since IP restoration schemes are still not well-known, the HSRP scheme will be used on an experimental basis. Future IP restoration schemes, if better than the HSRP scheme, may be considered for IP restoration.

Chapter 4

Survivability Approaches and Spare Resource Allocation for the SIAP

As described in Chapter 2, the future multiwavelength Optical Wide Area Networks (OWANs) will provide the capability of transporting different services like IP datagrams, ATM cells and SONET frames directly on different wavelengths of a WDM system. Since large amounts of data will be transported via fewer network elements in such a backbone network, many more customers may be affected by single failures, like a fiber cable cut, a cross-connect breakdown, etc. It is, therefore, imperative to provide a network infrastructure that is robust to failures and malfunctions of Network Elements (NEs) and is inherently self-healing to allow quick failure recovery. In order to ensure the survivability of the network, it is necessary to provide spare capacities (redundancies) for failure recovery. For a multi-service network like the one with SIAPs, spare capacity and restoration schemes may be assigned at different network layers, and for different network services. This increases the total cost of the network. It is important to design a survivable architecture for this network, which minimizes total cost while ensuring acceptable availability of services.

We consider two approaches for providing network protection. We also

describe two approaches for assigning spare capacity.

4.1 Survivability Approaches

In a general, multilayered network architecture, each network layer has a “client-server” relationship. This is illustrated in Figure 4.1. Consider a typical multilayered optical network that transports IP datagrams in ATM cells, that are carried within SONET frames, which in turn are transported over different wavelengths in a WDM system, as shown in Figure 4.1. It is clear that, in a typical failure scenario, if a single wavelength failure occurs, it results in loss of the SONET frames that are being carried on that wavelength. Each such failure in the SONET layer, in turn, leads to the loss of the corresponding set of ATM cells that the SONET frame transports. This further leads to the loss of even more IP datagrams. Thus, it is seen that failure propagates upward in network layers, with many more “clients” being affected by a single “server” failure.

In Chapter 3, we have already described the common failure restoration strategies at different network layers. In a multi-layered network, we need to determine at what layer, the restoration function should be performed. This decision has to be made such that the total spare capacity requirement (and hence the network cost) can be minimized while also minimizing the restoration time. In an architecture like the SIAP, it is possible to have different services directly being transported over WDM without the intermediate layering. In this case too, it is important to decide whether to perform the restoration functions at the service layer (i.e., the services affected perform the recovery function) or at the transport layer (i.e., the layer at which the failure actually occurs, performs the restoration function).

Based on this background, we now describe two approaches to network restoration. In Chapter 6, we shall discuss how each approach performs in

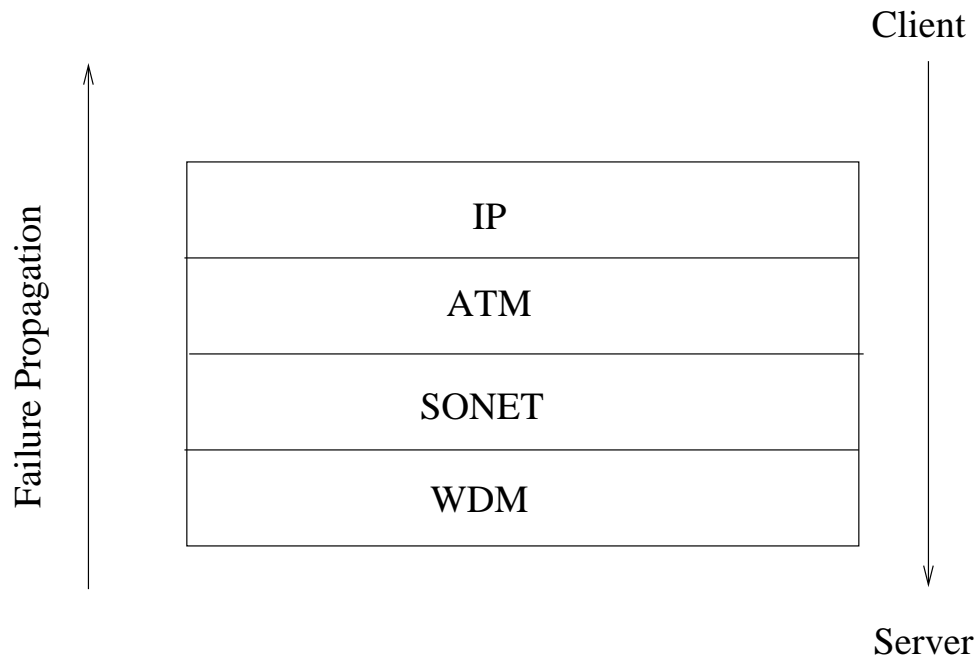


Figure 4.1: Typical multi-layered network with “Client-Server” relationship between network layers

terms of spare capacity requirements, network costs and restoration times for different network sizes, topologies and with different degrees of layering.

4.1.1 Service-Oriented Approach

In this approach to network survivability, the service that is affected by a failure, performs its own recovery function, irrespective of the origin of the failure. In a layered architecture, the highest layer that is affected by a failure, performs the restoration function. Thus, in a layered network architecture, shown in Figure 4.1, IP layer restoration (for example, using the Hot Standby Router Protocol (HSRP), described in Chapter 3) is performed, irrespective of whether the failure occurs due to an IP router failure, or an ATM switch failure, or a SONET ADM failure, or a WDM ADM failure, or even a fiber cut.

Similarly, in an ATM/SONET/WDM layered architecture, the ATM traffic is recovered using ATM VP restoration discussed in Chapter 3, regardless of the

origin of the failure. SONET native traffic is recovered using SONET recovery schemes that are suggested in Chapter 3. In the case of a service transparent network, where services are directly transported over WDM, as is possible with the SIAP architecture, this approach suggests that the affected services perform their own restoration function.

The advantages of the Service-Oriented approach are:

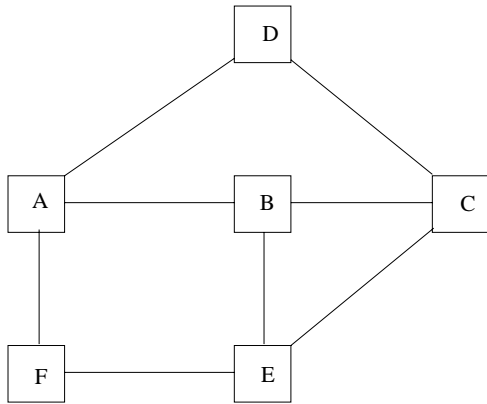
- Only a single recovery scheme is required to ensure survivability of traffic of a certain type. This means that inter-working of different survivability schemes in a layered architecture can be avoided. This simplifies the control and management functions required in the network.
- Since the transport network carries various classes of service, each with different survivability requirements, it seems easier to provide multiple degrees of reliability when the survivability is realized using the service-oriented survivability schemes.

This approach, however, has the following disadvantages:

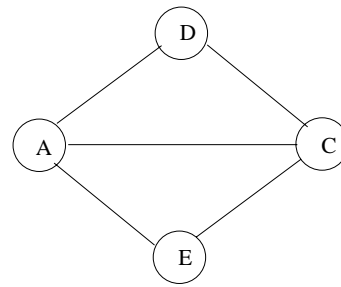
- As mentioned before, failure multiplication can occur very easily in layered networks because of the finer switching granularity of higher network layers. This can be seen in Figure 4.2.

Consider a physical topology as shown in Figure 4.2 (a). For the sake of simplicity, assume a two layer network, with the highest layer connectivity shown by the virtual topology of Figure 4.2 (b) as per the table shown in the figure.

In this example, suppose there is a physical link failure between nodes A and B. As per the virtual path to physical path mapping shown in Figure 4.2, a single link failure between A and B leads to two virtual path failures i.e., A-C and A-E. Thus, if the service-oriented approach is used, two higher layer restorations have to be performed for a single lower layer



(a) Physical Network Topology



(b) Virtual Network (with respect to highest layer)

Virtual Path	Physical Path
A-C	A-B-C
A-D	A-D
A-E	A-B-E
D-C	D-C
C-E	C-E

Figure 4.2: Example network topology

failure. This can be avoided, as will be seen in the transport-oriented approach, by performing “bulk” recovery at the layer where the failure originated.

- Another consequence of failure propagation to higher layers is that higher layer recovery schemes become more complex. It has to be assured that working and backup virtual paths are in physically diverse paths, else, it would be impossible to recover from a physical link failure. Thus, routing of higher layer paths needs to be correlated with lower layer connections.
- The correlation of higher layer paths with lower layer connections, in turn, implies that spare capacity allocation becomes difficult. It may be necessary to perform group recovery of higher layer connections on the same physical route. Failure recovery at the highest layer also implies that more spare capacity investment at lower layers is required. This is because, spare capacity needs to be provided for the physical path, as well as for the multiple higher layer connections affected by the physical path failure.

Thus, overall, the service-oriented approach seems to make sense if the traffic is affected by failure occurring at that service layer, and not at the lower layers. Thus, it also makes sense for networks that are transparent, and do not have intermediate layers between the service layer and the transport layer. We shall evaluate the service-oriented approach in Chapter 5, for both layered and non-layered networks.

4.1.2 Transport-Oriented Approach

In this approach, the lowest network layer where the failure originates is used to perform failure recovery. Thus, in a IP/ATM/SONET/WDM layered architecture, if there is a Wavelength Path failure, then Wavelength Path restoration

is triggered off (as described in Chapter 3). This would automatically restore the higher layer services affected by the WDM layer failure. Similarly, ATM VPs affected by a single SONET equipment failure, can be recovered in aggregate by a single SONET restoration.

With respect to Figure 4.2, let us say physical link A-B fails. The demand is re-routed via the backup physical path A-F-E-B. The virtual paths that are affected (A-C and A-E) are automatically restored by the physical re-routing. Thus, one single physical layer restoration can restore all the services affected by a single physical layer failure.

The advantages of the transport-oriented approach are, therefore :

- Coarser granularity at lower layers enables faster recovery of higher layers, because multiple higher layer failures can be remedied with a single lower layer restoration. Thus, no special precautions need to be taken at the service layers to cope with complex failure scenarios.
- Since the transport-oriented protection provides adequate resilience to higher layer paths routed along that layer, addition higher layer protection requires less spare capacity than the service-oriented approach. This means that there is less wastage of higher layer equipment resources by assigning spare capacities, which in turn leads to better utilization of resources.

This scheme, however, has its own disadvantages too:

- If we consider the IP/ATM/SONET/WDM example, we realize that, in this approach, there are four recovery schemes responsible for IP datagrams -
 1. WDM Virtual Wavelength Path restoration in the case of WDM equipment failure,

2. SONET path recovery schemes in the case of a SONET equipment failure,
3. ATM VP restoration in the case of ATM equipment failure, and
4. IP re-routing or HSRP, in the case of IP equipment failure

This requires additional functionality in the network to co-ordinate the recovery actions at the different layers. It is important not to trigger off, say, the ATM recovery scheme in the event of SONET equipment failure, since this might lead to conflicting recovery actions. This additional co-ordination or interworking functionality adds to the complexity of this recovery approach.

- Another issue to be considered here is the allocation of spare capacity. Going back to the IP/ATM/SONET/WDM example, since IP datagrams are recovered by four schemes, we need spare IP resources, as well as spare ATM VPs, spare SONET paths and spare Wavelength Paths. We shall look at resource provisioning and allocation of spare capacities in the next section.

4.2 Spare Capacity Allocation

In the transport-oriented survivability approach discussed above, the cost-effective provisioning of spare resources presents a tough problem. We now describe two ways to plan spare resources in a multi-layer network.

4.2.1 Layered Spare Capacity Assignment

This is the traditional approach to spare capacity assignment in layered networks. Redundancies are provided at each network layer in this approach. Consider a network that is layered as ATM/SONET/WDM. In the event of an

ATM equipment breakdown, backup VPs need to be provided at the ATM layer for all working VPs crossing the failed equipment. In addition to these spare resources at the ATM layer, we require SONET paths to carry the working as well as the backup VPs. In the event of a SONET equipment failure, it is necessary to provide a backup SONET path, plus spare capacity to protect the ATM demand being carried over the SONET path. This ATM demand includes the working as well as spare capacity assigned at the ATM layer. Similar spare capacity assignments need to be done at the WDM layer, in the form of spare Virtual Wavelength Paths for Wavelength Path Failure, plus spare capacity to protect the working, as well as the spare SONET paths in addition to spare capacity for the ATM demand.

The major drawbacks of this approach are as follows:

- Spare ATM resources are considered as “working” demand for the SONET layer, thus increasing the working resources at the SONET layer. Thus, more working resources need to be protected at the lower network layers, in order to provide for both working, as well as spare, higher layer resources.
- If we use the transport-oriented survivability approach described in the previous section, these spare higher layer resources, which become the “working” demand for the lower layers, are actually already protected against lower layer failures, because of the bulk restoration capability of the lower layer. Therefore, provisioning of spare resources at the lower network layer in order to accommodate spare resources at higher layers, becomes a “redundant redundancy”.
- Each spare resource pool is dedicated to a specific network layer recovery scheme and cannot be shared across network layers. This means to say, SONET spare resources cannot be used to perform ATM recovery func-

tions or vice versa. Thus a lot of spare capacity is wasted.

Thus, in general, the traditional layered spare capacity provisioning concept requires an excessive amount of spare resources overall.

4.2.2 Pre-emptive Spare Capacity Assignment

This spare capacity assignment scheme was proposed at the University of Ghent [15]. In this approach, higher layer spare resources are supported as traffic that can be “pre-empted” by lower layer spare resources. This enables the re-use of lower layer spare resources to carry higher layer spare resources. This helps resolve the “redundant redundancy” problem mentioned above.

Going back to our ATM/SONET/WDM example of the previous section, the total needed spare resources can be decreased by re-using the SONET capacity occupied by spare ATM resources, for SONET recovery purposes. These spare ATM resources are useful for ATM recovery in the event of ATM equipment failure, but are useless in the event of SONET equipment failure, when we use the transport-oriented survivability approach. This is because, SONET recovery schemes are used to restore ATM services when the SONET equipment fails. In the pre-emptive spare capacity scheme (also called the *Common Pool* scheme in [15]), the SONET capacity occupied by the ATM spare resources, is utilized by SONET recovery schemes. The spare resource sharing can be achieved by making higher layer spare resources “pre-emptible” in the event of lower layer equipment failure, i.e., if there is a SONET equipment failure, the spare capacity allocated at the ATM layer (for ATM equipment failures) is pre-empted and allocated to the SONET layer. It should be noted that the pre-emptive spare capacity assignment scheme is applicable only in conjunction with the transport-oriented survivability approach. In the case of the service-oriented survivability approach, the ATM resources are still required even in

the event of SONET or WDM equipment failures, and hence, must not be pre-empted.

Another issue in this scheme is to plan higher layer spare resources to use separate ports of their cross-connects (or switches, routers, add-drop multiplexers as the case may be). For instance, working VP connections and spare VPs should use separate ports of an ATM switch. This ensures that spare and working resources of the ATM logical network are treated in a different way by the underlying transport network. This also allows for the planning of the transport network to be different and therefore, results in cost savings at the transport layer. In other words, the working resources in the transport layer (say SONET paths) carry native SONET demand as well as ATM working resources, but not the spare ATM resources. The spare SONET resources protect the working SONET resources (including the ones carrying ATM traffic). A few, if any, additional resources will then be required at the SONET layer to protect ATM spare resources.

A further implication of the pre-emptive resource sharing scheme is that, because higher layer spare resources can be pre-empted by lower layer resources, in the event of lower layer failures, some part of the higher layer spare resources may be unavailable temporarily until the lower layer failure is repaired. (i.e., spare ATM resources may be unavailable during a SONET equipment failure). This, however, does not affect the higher layer survivability, as these services are automatically restored using the transport-oriented survivability approach. Thus, the major advantage of this scheme is the re-use of spare lower layer resources to provide “extra” survivability at the higher layer.

An important issue to successfully deploy this scheme is to translate spare capacity requirements of different layers in terms of a common unit, so that resource sharing can be employed using a common pool. As will be seen in Chapter 5, we have opted to translate all spare capacities to Virtual Wavelength

Paths, as these are the basic resources used in the WDM transport network for the SIAPs.

Precautions need to be taken to prevent higher layer recovery schemes from being activated in the event of higher layer traffic being affected on account of lower layer failures. This requires alarm correlation schemes as well as synchronization schemes.

4.3 Summary

The taxonomy of the different survivability approaches, spare capacity schemes and network architectures discussed in this chapter is shown in Figure 4.3.

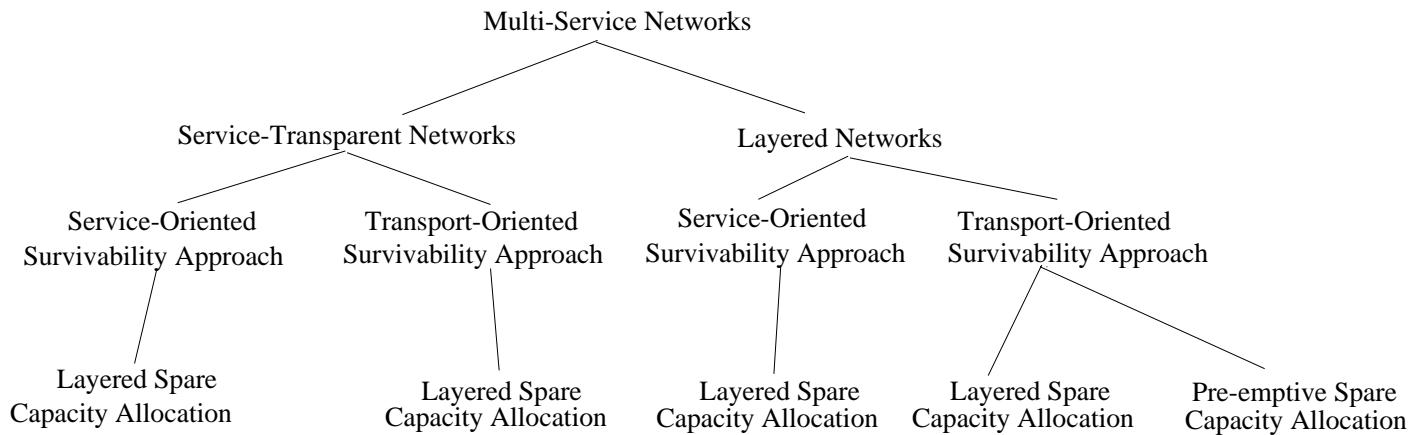


Figure 4.3: Taxonomy of Network Architectures, Survivability Approaches and Spare Capacity Allocation Schemes

Chapter 5

Analysis Methodology, Performance Evaluation of Different Survivability Approaches

In this chapter, we describe a general framework to evaluate the performance of different survivability architectures, based on the network cost (in terms of the amount of spare resources required) and the restoration time for different failure scenarios. A quantitative measure of the network survivability is provided.

Different approaches to quantify the network resilience have been proposed [6, 4, 2]. In [6], an analysis of the service unavailability for different network architectures and restoration schemes, based on the modeling of self-healing architectures, is presented. A framework for disaster-based network survivability, wherein survivability is characterized in terms of a “survivability density function”, is presented in [4]. Our approach to quantifying the network survivability is motivated by [2]. In [2], the degree of survivability is measured in terms of the fraction of the total service demand (before failure) that is available after a failure event and the remedial action that is taken thereafter. This frac-

tion also includes the services that are not affected by the failure. For example, if the total demand before a failure event is, say, 10 (in arbitrary units). After a failure occurs, if the demand that is unaffected is 3. If the restored demand after failure is 4, then the total available demand after the remedial action is $3 + 4 = 7$. Thus the degree of survivability, according to [2] becomes $\frac{7}{10} = 0.7$.

In our approach, we do not consider the demand that is not affected by the failure to be part of the measure of the degree of survivability. This is because, we are interested in evaluating different survivability approaches to restore *affected* demand only. Thus, in the previous example, the degree of survivability according to our definition becomes the ratio of restored demand to affected demand, i.e., $\frac{4}{6} = 0.67$.

5.1 Network Survivability Analysis

5.1.1 Degree of Survivability

In order to quantitatively measure the fault-tolerance of the network and the effectiveness of the restoration scheme used, we define a parameter $s(t)$ as the *degree of survivability*. The degree of survivability, as we define it, is the ratio of restored demand to the affected demand, in the event of a failure. Thus, s varies from 0 to 1. As is clear by the notation, $s(t)$ is a function of time t .

The nature of $s(t)$ is shown in Figure 5.1. Thus, as soon as the network failure occurs, at time $t = 0$, s drops to zero. The time required for the failure information to propagate after the failure is detected is shown as t_{det} . The restoration time t_r required to attain a target survivability s_T is dependent on the size of the network, the distance between the node pairs (or the link lengths), the amount of spare resources allocated and the restoration schemes used. The time for complete restoration of all services is t_R . Thus, $s(t_R) = 1$.

For $s(t_r) = 0$, there is no redundancy or protection from failure in the network,

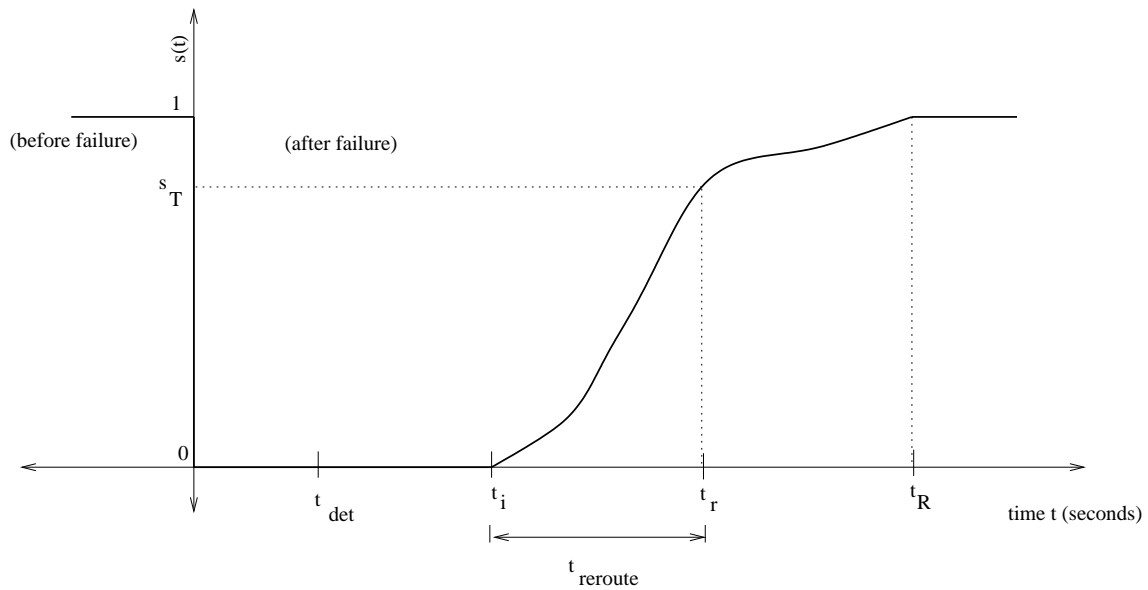


Figure 5.1: Degree of survivability $s(t)$

as a result of which, the services affected are irrecoverable. This is the worst case, but it has the minimum cost, since no protection mechanisms are provided for.

On the other hand $s(t_r) = 1$ ensures that the network is completely survivable against failure. In this case, $t_R = t_r$. This represents the most desirable case. However, the costs involved in ensuring complete survivability may be high, and it may also take a lot of time to restore all the affected services completely.

5.1.2 Restoration Time

The total restoration time t_r required to attain a target survivability s_T is composed of [2]:

- Detection time - the time taken to detect the failure.
- Notification time - the time taken to notify all the nodes in the network of the failure. This includes the propagation delay (which depends on the

inter-node distances) as well as the per-node processing time.

- Affected service identification time - the time taken to identify the services affected by the failure.
- Path selection time - the time taken to select alternate routes for the affected services. This time can be avoided by pre-planned allocation of spare routes.
- Rerouting time - the time taken to reroute the affected services using the spare paths so as to attain the target survivability s_T .

Note 1: In our analysis, we express the affected demand in terms of the number of VWPs that are affected by the failure. Consequently, the restored demand is the number of VWPs that are restored. The rerouting time is the time required to restore the number of VWPs required to attain the target survivability s_T (i.e., the number of VWPs required is s_T times the number of VWPs affected by the failure).

Note 2: For the purpose of comparing the various survivability schemes, we assume that one logical path for each kind of service is mapped on to one VWP, i.e., for example, one SONET path is mapped on to one VWP and so is one ATM VP, and so also one IP “flow”. This is based on the assumption in [3], where an ATM VP is mapped on to a VWP in an ATM-based photonic network.

Note 3: In this analysis, we have taken the restoration times assuming the worst-case scenario that processing of link failure cannot be done in parallel, and each node needs to be informed about the failure through the physical layer topology.

We now discuss the typical restoration times for Virtual Wavelength Path Restoration at the WDM layer [3], the SONET Self Healing Ring and/or Automatic Protection Switching scheme [1], the ATM VP restoration scheme [8] and the Hot Standby Router Protocol for IP Router Failure restoration [12].

5.1.2.1 VWP Protection

- A failure is detected when there is no signal on a particular wavelength channel. This is equal to the length of time required to transmit an optical frame, t_{frame} which is equal to $125\mu\text{s}$.
- If N_w nodes are to be informed about the failure, and the average inter-node distance is l km, the total propagation delay for failure notification is $\frac{N_w l}{2 \times 10^5}$ seconds where the denominator is the speed of light through fiber in kilometers per second. The per-node processing delay, $t_{\text{proc}}^{\text{WDM}}$ in WADM is currently approximately 3ms [3]. Thus the total time required to notify other nodes of the failure is $\frac{N_w l}{2 \times 10^2} + N_w \times t_{\text{proc}}^{\text{WDM}}$ milliseconds.
- By assigning alternate VWPs and spare capacity in advance, we eliminate the need for dynamic path selection.
- Suppose the affected WDM demand is D_{aw} VWPs. If the required degree of survivability is s_T (which by definition is the ratio of the restored demand to affected demand), the number of VWPs to be restored is $s_T \times D_{\text{aw}}$. The switching time, $t_{\text{sw}}^{\text{WDM}}$ per VWP is typically 20 ms or faster[3]. Thus the rerouting time is $t_{\text{sw}}^{\text{WDM}} \times s_T \times D_{\text{aw}}$.

The total restoration time in milliseconds to restore WDM services is given by:

$$t_r^{\text{WDM}} = t_{\text{frame}} + \frac{N_w l}{2 \times 10^2} + (N_w \times t_{\text{proc}}^{\text{WDM}}) + (t_{\text{sw}}^{\text{WDM}} \times s_T \times D_{\text{aw}}) \quad (5.1)$$

5.1.2.2 SONET Protection

- A failure is detected when there is an Alarm Indication Signal (AIS) indicating Loss of Signal (LOS), Loss of Frame (LOF) etc. The time required to detect a failure, $t_{\text{det}}^{\text{SONET}}$, (or a signal degrade such that the Bit Error Rate is greater than 10^{-6}) is about 10 ms [1, 8].

- If N_s nodes are to be informed about the failure, and the average inter-node distance is l km, the total propagation delay for failure notification is $\frac{N_s l}{2 \times 10^5}$ seconds where the denominator is the speed of light through fiber. The per-node transfer delay is due to the fact that 3 consecutive SONET frames (K1 and K2 bytes) indicating the failure state have to be received. The processing delay is, therefore, equal to $3 \times 0.125 = 0.375$ ms. The processing delay per node is $125 \mu\text{s}$. For bidirectional switching, this delay is multiplied by two (i.e., $250 \mu\text{s}$). The processing delay, $t_{\text{proc}}^{\text{SONET}}$ is, therefore, equal to $0.375 + (N_s \times 0.250)$ ms per K1/K2 byte transfer. Three such transfers are required for successful switching. Thus the total time required to notify other nodes of the failure is $\frac{N_s l}{2 \times 10^2} + (3 \times t_{\text{proc}}^{\text{SONET}})$ milliseconds.
- By assigning alternate demand paths and spare capacity in advance, we eliminate the need for dynamic path selection.
- Suppose the affected SONET Demand is D_{as} VWPs. As explained in **Note 2** above, we assume that one SONET path is transported on a single VWP. If the required degree of survivability is s_T , the demand, in terms of number of VWPs to be restored is $s_T \times D_{as}$ per link. The switching time, $t_{\text{sw}}^{\text{SONET}}$ per VWP is typically 10 ms or faster. Thus the rerouting time is $t_{\text{sw}}^{\text{SONET}} \times s_T \times D_{as}$.

The total restoration time in milliseconds to restore SONET services is given by:

$$t_r^{\text{SONET}} = t_{\text{det}}^{\text{SONET}} + \frac{N_s l}{2 \times 10^2} + (3 \times t_{\text{proc}}^{\text{SONET}}) + (t_{\text{sw}}^{\text{SONET}} \times s_T \times D_{as}) \quad (5.2)$$

5.1.2.3 ATM Protection (from [8])

- It is shown [8] that the time, $t_{\text{det}}^{\text{ATM}}$, required to detect a “hard” failure ($\text{BER} > 10^{-3}$) in an ATM network, with link rate 2.4 Gbps, is currently about 0.1 ms.

- If N_a nodes are to be informed about the failure, and the average inter-node distance is l km, the total propagation delay for failure notification is $\frac{N_a l}{2 \times 10^5}$ seconds where the denominator is the speed of light through fiber. The per-node processing delay in ATM switches, t_{proc}^{ATM} is typically 1 ms. Thus the total time required to notify other nodes of the failure is $\frac{N_a l}{2 \times 10^5} + N_a \times t_{proc}^{ATM}$ milliseconds.
- By assigning alternate VWPs and spare capacity in advance, we eliminate the need for dynamic path selection.
- Suppose the affected ATM demand is D_{aa} VWPs. If the required degree of survivability is s_T , the number of VPs to be restored is $s_T \times D_{aa}$. As per **Note 2** above, we make the simplifying assumption that one VWP carries a single VP. The time required to activate a single VP, t_{VP} is typically 0.1 ms[8]. Thus the rerouting time is $t_{VP} \times s_T \times D_{aa}$.

The total restoration time in milliseconds to restore ATM services is given by:

$$t_r^{ATM} = t_{det}^{ATM} + \frac{N_a l}{2 \times 10^5} + (N_a \times t_{proc}^{ATM}) + (t_{VP} \times s_T \times D_{aa}) \quad (5.3)$$

5.1.2.4 IP Protection

- In the HSRP protocol [12], periodic HELLO packets are sent in each logical route to see if the route is available. This HELLO time is configurable. The minimum time required to detect a failure is, therefore, a HELLO interval. A typical value[12] of the HELLO time is $t_{HELLO} = 1$ second.
- The time taken to declare a router to have failed, is the HOLD time. This is typically set to $t_{HOLD} = 3$ seconds[12]. If N_i nodes are to be informed about the failure, the total time required to notify each affected node about the failure is $N_i \times t_{HOLD}$ seconds.

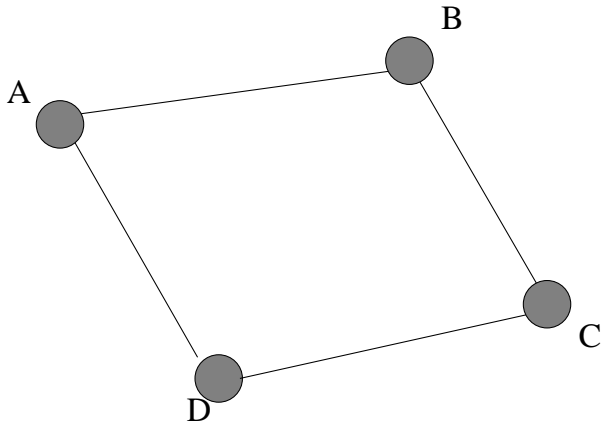
- By assigning alternate routes and spare capacity in advance, we eliminate the need for dynamic path selection.
- Suppose the affected IP demand is D_{ai} VWPs. As explained in **Note 2** above, we assume that one VWP carries a single IP "flow" path. If the required degree of survivability is s_T , the demand, in terms of number of VWPs to be restored is $s_T \times D_{ai}$ per link. The rerouting time per new route is typically $t_{reroute} = 12$ seconds[12]. Thus the rerouting time is $t_{reroute} \times s_T \times D_{ai}$ seconds .

The total restoration time in seconds to restore IP services is given by:

$$t_r^{IP} = t_{HELLO} + \frac{N_i l}{2 \times 10^5} + (N_i \times t_{HOLD}) + (t_{reroute} \times s_T \times D_{ai}) \quad (5.4)$$

5.1.3 Demand Requirements

In order to make the framework independent of bit-rates, we consider the basic unit of capacity as one Virtual Wavelength Path (VWP). A VWP can carry SONET frames, ATM VPs, IP datagrams or any other data format. Bandwidth can be assigned to VWPs just like it is assigned to ATM VPs. Spare capacity requirements of different network services can be expressed in terms of the number of VWPs required to transport those services. Another reason for expressing capacity in terms of VWP's is that these can easily be expressed in terms of number of SONET DS3s (or equivalent), or ATM VP bandwidth or simply bits per second, as and when it is desired, if we know the capacity of the service path being considered. For example, if we know that one VWP carries a single SONET path, which is allocated a bandwidth of 10 DS3s, then we know that the capacity of a VWP carrying SONET is equivalent to 10 DS3s. Similarly if the pre-allocated ATM VP bandwidth for a given connection is 40 Mb/s, then the VWP carrying an ATM VP has a capacity of 40 Mb/s. The maximum capacity of any VWP is the available link rate.



(a) Example Network

Node Pair	Demand	Route
(A,B)	4	A-B
(A,C)	3	A-D-C
(B,D)	4	B-C-D
(C,D)	5	C-D

(b) Demand pairs and Routing Table

Link	Dropped Demand	Transit Demand
AB	4 (A,B)	-
BC	-	4(B,D)
CD	3(A,C) + 4(B,D) + 5 (C,D)	-
AD	-	3(A,C)

(c) Dropped Demand and Transit Demand of Links

Figure 5.2: Illustration of Dropped and Transit Demand

Each link has some *transit demand* and some *dropped demand*. The transit demand for any link is the demand that traverses either node of the link as an intermediate hop before the actual destination. The dropped demand is the demand that is destined for any end-node of the link (i.e., it is dropped at that node and not carried over to the other nodes). This is illustrated in Figure 5.2. In the example network of Figure 5.2 (a), let us consider link AB. This link carries the demand for demand pair (A,B) = 4, as seen in Figure 5.2 (b). This is *dropped* demand, as it is not carried over beyond node B. Now consider link BC. This link carries *transit* demand between nodes B and D. This transit demand (4 units) is not dropped at C, but carried over to link CD. However, since it is *dropped* at D, the demand for node-pair (B,D) becomes part of the *dropped* demand for link CD. Link CD also carries dropped demand between node pairs ((A,C) (3 units) and (C,D) (5 units). Similarly, link AD carries transit demand of 3 units attributed to node pair (A,C). The dropped and transit demands for the four links of the network are shown in Figure 5.2 (c).

For a network with N nodes, as per our formulation, we define the following parameters:

- d_{ij} → VWP demand between nodes i and j . Thus d_{ij} is the *dropped demand* at node j from node i .
- p → Spare capacity ratio, i.e., the ratio of required spare capacity to the corresponding working capacity
- q → Transit capacity ratio, i.e., the ratio of transit VWP demands to dropped VWP demands at each node.

Thus, the total number of working VWPs dropped at each node i is the sum of all the VWP demands destined for that node from every other node. This is given by the summation :

$$\sum_{\substack{j=1 \\ j \neq i}}^n d_{ij}$$

The total number of VWPs terminated at each node is the sum of the total dropped demand and the total transit demand at that node. Using the definition of the transit capacity ratio q described above, we get:

$$\begin{aligned} & \text{Total working VWP demand terminated at each node } j \\ &= \text{Total dropped VWP demand} + \text{Total transit VWP demand} \\ &= (1 + q) \sum_{\substack{j=1 \\ j \neq i}}^n d_{ij} \end{aligned}$$

The total VWP demand requirement at each node j is the sum of the working demand and the protection demand. Using the spare capacity ratio p defined above, we have:

$$\begin{aligned} & \text{Total VWP demand terminated at each node } j \\ &= \text{Total working VWP demand} + \text{Total spare VWP demand} \\ &= (1 + p)(1 + q) \sum_{\substack{j=1 \\ j \neq i}}^n d_{ij} \end{aligned}$$

The network cost is directly related to the total demand requirement (dropped plus transit) at each node of the network. In addition to the variable transport cost of the VWPs in the network, we have fixed costs like the cost of fiber and the network equipment used. For a given network topology, we can determine the fixed costs and express these in terms of VWP demand requirements. The variable transport cost depends on the survivability and spare capacity assign-

ment approach, as also the degree of transparency of the network. Knowing the demand pattern of a given network and the transit and spare capacity ratios, the variable transport cost can be evaluated. Since the network cost is directly related to the capacity requirements, we shall limit our discussion to determining the capacity requirements, as an indicator of network cost. For a required degree of survivability s_T for a given failure condition, we can obtain the relationship between s_T and capacity r . Using this information we can also find out the restoration time t_r for attaining a target survivability s_T for a particular restoration scheme.

5.1.4 Comments about parameters p and q

By introducing the Spare Capacity Ratio p , and the Transit Capacity Ratio q , we have made this framework very general and adaptable to any kind of network topology and any survivability strategy.

The parameter p varies according to the network connectivity and survivability approach used. In general, for highly connected mesh networks, $p \rightarrow 0.5[1]$.

The parameter q depends on the extent of network connectivity. If every node of the network is connected to every other node, then there is no transit demand at any node, as direct links are available from point-to-point. Thus, for a fully interconnected mesh architecture, $q = 0$. Similarly, in the case of a Ring demand pattern, the transit demand at each node is almost always equal to the total demand that is dropped at that node. Hence, $q = 1$ for ring-connected demand patterns.

5.1.5 Algorithm to Evaluate the Performance of Survivability Approaches

Let us consider a hypothetical network of N nodes. We define additional parameters below in order to generalize this framework to any network topology and size.

In this framework, we define:

- Let $M = \{m_1, m_2, m_3 \dots m_n\}$ be the set of different survivability approaches.
- The total spare capacity requirement is r . For this framework, we define the units of spare capacity in terms of the number of Virtual Wavelength Paths required. This makes the parameter bit-rate independent.
- The total network cost is directly related to the total capacity requirements (working and spare). In addition, the network cost includes the initial investment cost and the transport cost. We shall, however, discuss only the capacity requirement for each link in the network in order to support the working and the spare demand to ensure the required degree of survivability.
- The restoration time is described by t_r . This is the time required to restore the failed services in order to attain a target survivability of s_r .

For each survivability approach $m_k \in M$, we need to determine the total capacity requirement of the network in order to meet the s_r survivability degree and measure the corresponding restoration time t_r . We summarize the methodology to analyze the survivability of any network, for a given demand pattern, connectivity and transparency. It should also be noted that this framework is equally applicable to smaller networks as it is applicable to Wide Area Networks.

- For a given physical network topology, establish the logical topologies for the different services/layers supported by the network (for example, the physical connectivity could be in the form of a ring network, but the logical connections, like the ATM VP connections or the IP flows or the WDM VWPs may have different topologies, like mesh, supercube, hypercube etc). Logical topologies should be designed such that the shortest physical path is chosen to interconnect the nodes forming the logical links, and, at the same time, the mapping of the logical topologies to the physical topology should be such that resource blocking is avoided as far as possible. In a WDM logical network (i.e., a logical “network” formed by interconnecting different VWPs), resource blocking refers to wavelength blocking - which means that the number of wavelength channels required in any physical link in order to satisfy a particular logical connection, exceeds the number of wavelengths available. In an ATM network, resource blocking refers to excessive bandwidth requirements of VPs. In general, the total bandwidth required on any link should not exceed the available link capacity. The design of logical topologies for wavelength-routed optical networks is discussed in [30]. The design of the optical layer is discussed in [31] and the wavelength assignment problem is addressed in [32].
- The next step is the Demand Assignment. For a given network, the demand pattern is usually known. Else, for the purpose of analysis, a demand pattern between each node pair is established for the physical as well as logical topologies being considered. The transit capacity ratio q is determined based on the network connectivity. This is then used to compute the total capacity for each logical link for each logical topology. The mapping of the logical topologies to the physical topology yields the total working capacity for each physical link.

- A list of all possible, or most frequently occurring failure scenarios (like a fiber cut, a Network Element (SONET ADM, ATM switch, IP router, WADM etc.) failure, etc.). Alternatively, if we wish to compare survivability approaches for only a particular kind of failure, like single physical and logical link failures, only those scenarios are listed.
- For each failure scenario from the above list, we consider different survivability approaches and spare capacity assignment strategies. In the present work, we limit the survivability approaches to the Service-Oriented and Transport-Oriented approaches discussed in Chapter 4. The spare capacity assignment strategies used are the Layered approach and the Pre-emptive approach, as described in Chapter 4.
- For each such approach
 - The spare capacity is assigned to each logical and physical link to achieve the desired degree of survivability s_T . The spare capacity ratio p is then calculated and the spare capacity r is determined for each link.
 - The total VWP demand (including both the working as well as the spare demand) for each logical network link is computed. Based on the survivability approach and the spare capacity assignment approach used, these demands are mapped to each physical link.
 - The restoration time t_r for this s_T is estimated using the relationship between restoration time and demand to be restored for different restoration schemes, as already discussed in Section 5.1.2. (From Figure 5.1, $s_T = 1$ implies $t_r = t_R$).
 - The above calculations are repeated for a given $t_r < t_R$ constraint and the corresponding s_T is determined (in this case the spare ca-

capacities are assigned taking into account 100% survivability and the restoration time to achieve 100% survivability, t_r is calculated).

- Comparative plots and tables are generated to evaluate $s(t)$, r and t_r
- The most cost-effective and fast-restoring survivability approach is recommended for the given network topology and degree of transparency.

The above algorithm is summarized in the flow diagram shown in Figure 5.3.

5.2 A Simple Example to Illustrate the Algorithm

We first consider a simple four-node network, shown in Figure 5.4 in order to illustrate the application of the algorithm formulated in the previous section. The survivability analysis of this network is done as per the steps described in the previous section. After understanding the algorithm, we proceed to analyze a more practical, larger network in the next section. We consider a simple hypothetical network that has ATM and SONET services over WDM.

5.2.1 Topology

As shown in Figure 5.4 (a), we have the physical (or WDM layer) connected in a ring topology. Figure 5.4 (b) and (c) show the logical topologies formed by point-to-point path connections at the ATM and SONET layers respectively.

5.2.2 Demand Assignment

The next step, after establishing the physical and logical topologies of the network is Demand Assignment. Let us first consider the demand assignment at the ATM layer. Let us suppose that each node pair carries the same demand, equivalent to one VWP. From Figure 5.4 (b), it is clear that the logical ATM

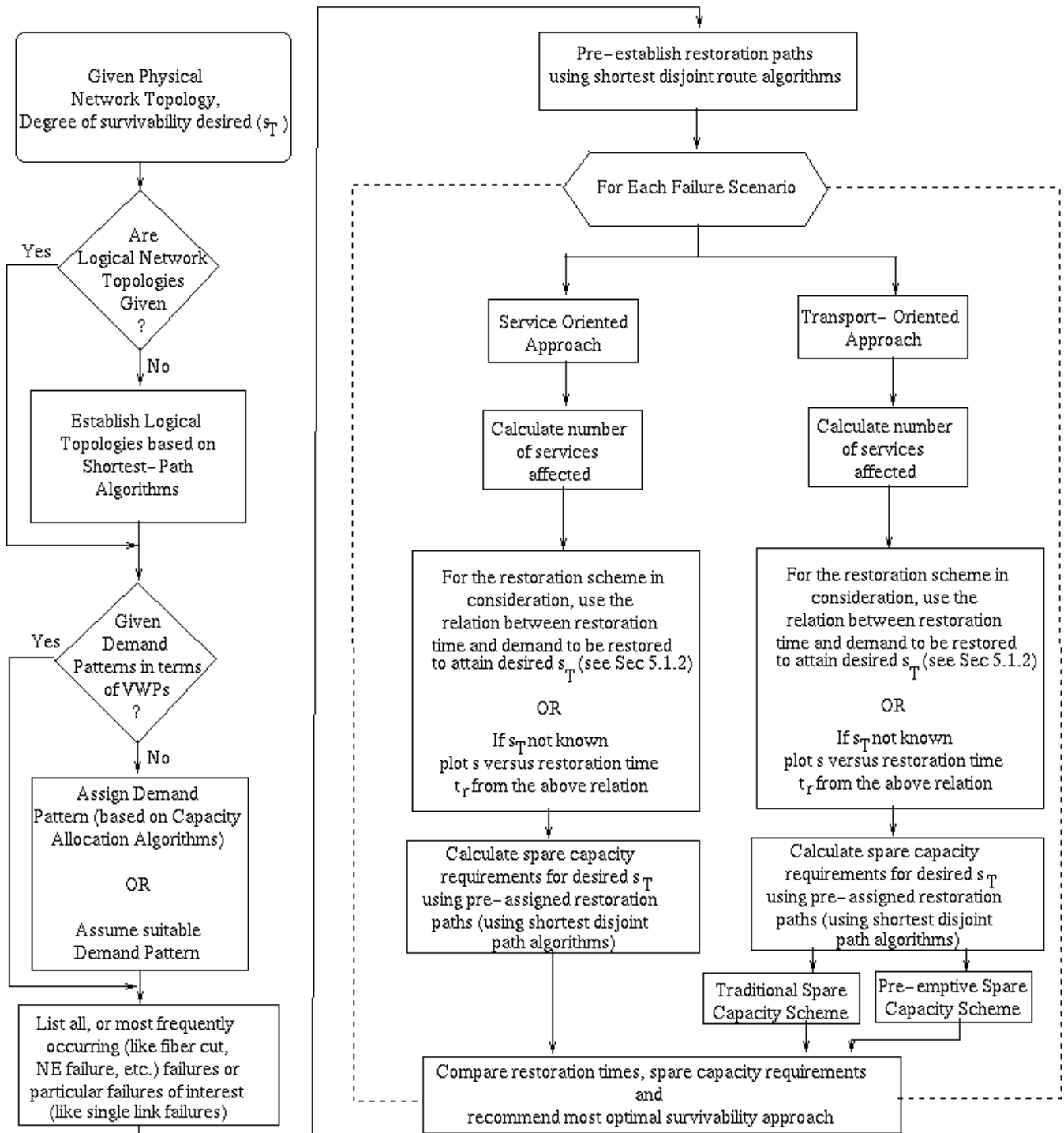


Figure 5.3: Flow Diagram for the Algorithm to evaluate different survivability schemes

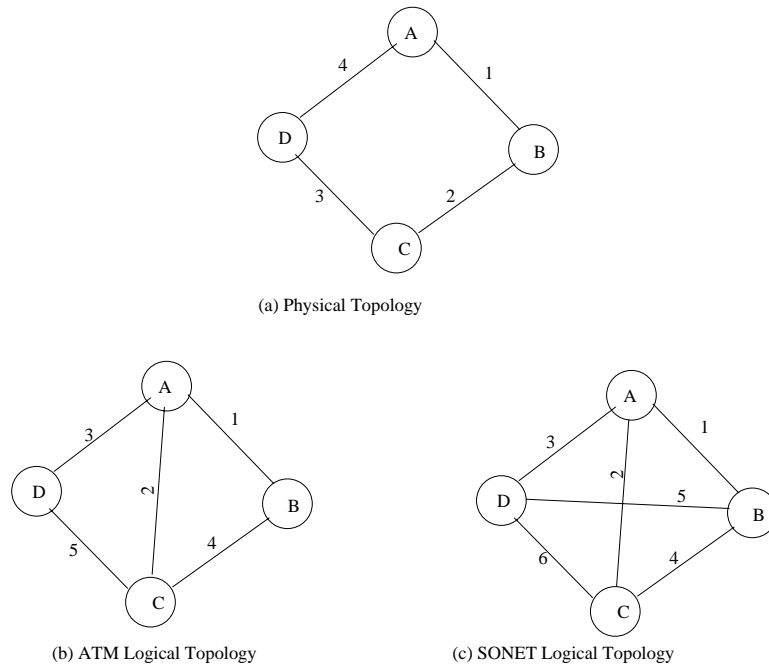


Figure 5.4: Simple Example Network - Physical and Logical Topologies

topology provides a direct logical path (a VP in this case) for each demand pair, except for the demand between nodes B and D. Let us consider that the ATM demand between nodes B and D traverses node C, i.e., it is mapped on to logical paths BC and CD. As per our definition, this constitutes some transit demand over logical link BC and is dropped on link CD. The working demand distribution for each ATM logical link is tabulated in Table 5.1.

Table 5.1: ATM logical layer (4 node network) - demand pattern

Logical Link	Dropped Demand	Transit Demand	Total Demand
AB	1	0	1
AC	1	0	1
AD	1	0	1
BC	1	1 (for (A,D))	2
CD	2 (incl. (A,D))	0	2

From Figure 5.4 (c), it is clear that the SONET logical network forms a fully interconnected mesh. Thus, there exists a direct logical path for each demand pair, and, therefore, there is no transit demand associated with any logical link.

Each logical link in the SONET network carries a demand of one VWP.

Now, let us consider the mapping of each logical layer to the physical layer network.

1. Service-transparent Network

If we consider a service-transparent network, then both the ATM logical network as well as the SONET logical network are directly mapped on to the WDM physical layer network. In this case, the mappings for the ATM network to the physical layer and the SONET network to the physical layer are shown in Table 5.2 and Table 5.3 respectively.

Table 5.2: ATM logical layer to Physical layer mapping (4 node network)

Logical ATM Link	Physical Link
AB	AB
AC	AB, BC
AD	AD
BC	BC
CD	CD

Table 5.3: SONET logical layer to Physical layer mapping (4 node network)

Logical SONET Link	Physical Link
AB	AB
AC	AB, BC
AD	AD
BC	BC
BD	BC, CD
CD	CD

For a more complicated, realistic network with multiple services, the demand routing is done using well known algorithms that select the shortest available path. The logical to physical layer mappings are also done such that there is no resource blocking on the links. Spare capacity assignments are done based on the degree of survivability required. In order to avoid the overhead of dynamic spare route calculation, spare paths are

usually pre-assigned. These spare paths are assigned such that route diversity is achieved.

Based on the above mappings, the working demand requirement for each physical link are calculated. Thus, physical link AB accommodates ATM logical paths AB and AC. It also accommodates SONET paths AB and AC. Each of the above paths has a VWP requirement of 1. Thus, physical link AB has a working requirement of 4 VWPs. Similarly the working requirements of the other physical links (BC, CD and AD) are calculated and tabulated in Table 5.4.

Table 5.4: Physical layer working demand requirements (service-transparent network)

Physical Link	ATM Demand	SONET Demand	Total Demand
AB	1 (AB) + 1 (AC)	1 (AB) + 1 (AC)	4
BC	1 (AC) + 2 (BC)	1 (AC) + 1 (BC) + 1 (BD)	6
CD	2 (CD)	1 (BD) + 1 (CD)	4
AD	1 (AD)	1 (AD)	2

2. Layered network

In the case of the layered network, ATM services are mapped on to the SONET layer which is then mapped on to the WDM layer. In this case, the SONET logical links carry ATM demand in addition to the SONET native demand. The working demand requirements at the SONET layer, are, therefore increased. The working demand requirements at the SONET layer for the layered 4 node network are tabulated in Table 5.5.

Table 5.5: SONET layer working demand requirements (layered network)

SONET Logical Link	ATM Demand	SONET Demand	Total Demand
AB	1 (AB)	1 (AB)	2
AC	1 (AC)	1 (AC)	2
AD	1 (AD)	1 (AD)	2
BC	2 (BC)	1 (BC)	3
BD	-	1 (BD)	1
CD	2 (CD)	1 (CD)	3

The physical layer requirements for the layered network are shown in Table 5.6.

Table 5.6: Physical layer working demand requirements (layered network)

Physical Link	SONET Native Demand	SONET Layer ATM demand	Total Demand
AB	1 (AB) + 1 (AC)	1 (AB) + 1 (AC)	4
BC	1 (AC) + 1 (BC) + 1 (BD)	1 (AC) + 2 (BC)	6
CD	1 (BD) + 1 (CD)	2 (CD)	4
AD	1 (AD)	1 (AD)	2

5.2.3 Failure Scenarios

Since this is an illustrative example network, we shall not consider all possible link failures. Let us consider the following situations separately :

1. Physical Link CD fails (for e.g., due to a fiber cut)
2. Logical SONET link BC fails (for e.g., due to failure of the SONET equipment connecting B and C)
3. Logical ATM link BC fails (for e.g., due to failure of a port of the ATM switch that establishes the VP between B and C)

We are not concerned about what equipment failure actually causes the above physical or logical links to be inaccessible. To simplify our analysis, we shall treat any kind of failure in terms of the physical and/or logical link failures that result from it.

5.2.4 Survivability analysis

5.2.4.1 Service-Oriented Approach

As mentioned before, in the Service Oriented Approach, the services that are affected by a particular failure, perform the restoration function, irrespective of the origin of the failure.

1. Failure of Physical link CD

From Table 5.4, for the service-transparent network, the failure of physical link CD affects the ATM demand carried on ATM logical link CD (2 VWPs) as well as the SONET demand carried on SONET logical links BD and CD (1 VWP each). Using the service-oriented approach, this means that two restoration schemes - one at the ATM layer and another at the SONET layer - would be needed to restore the affected services.

Let us suppose that we have an average link length of 100 km. Since it is a 4-node network, the failure message needs to be propagated to 2 nodes (since the other 2 nodes constitute the link that has failed). If 100 % survivability is desired, i.e., target survivability $s_T = 1$, then, using Equation 5.2 for SONET restoration and the typical values of the variables listed therein, we have :

$$\begin{aligned} t_r^{\text{SONET}} &= 10 + \frac{(2 \times 100)}{2 \times 10^2} + 3(\times (2 \times 0.250) + 0.375) + (10 \times 1 \times 2) \\ &= 33.625 \text{ms} \end{aligned}$$

If, however, we desired only 50 % survivability, then substituting $s_T = 0.5$ in Equation 5.2, we can calculate the restoration time for SONET services to be 23.625 milliseconds.

Similarly, using Equation 5.3, we can compute the time required to completely restore the affected ATM services. $t_r^{\text{ATM}} = 0.1 + \frac{(2 \times 100)}{2 \times 10^2} + 2 + (0.1 \times 1 \times 2)$
 $= 3.3 \text{ms}$

If only 50 % restoration is desired, the restoration time for ATM services becomes 3.2 ms. It can thus be seen that ATM restoration is extremely fast as compared to SONET restoration (as expected). It is also interesting to observe that the difference in restoration time between complete restoration and 50 % restoration of ATM services is only 0.1 ms. Thus, we can expect a very steep slope (almost vertical) when we plot the degree of survivability for ATM restoration versus the restoration time.

From Tables 5.4 and 5.6, we observe that for the example network being considered, the number of services affected by the failure of any physical link is the same for the service-transparent as well as the layered networks. Hence, the restoration times will also be the same. It should, however, be noted that in practical cases, the demand requirements for a layered network may differ from the service-transparent network, and so the calculations must be repeated.

2. Failure of logical SONET link BC

In the service-transparent network, the failure of logical SONET link BC leads to 1 VWP (demand between B and C) being lost. Repeating the calculations for an average link length of 100 km, using Equation 5.2, the restoration time for complete restoration can be calculated to be 23.625 ms. Since there is only 1 VWP to be restored, the degree of survivability can have a value of 0 (no restoration) or 1 (restoration of the only VWP). In the case of the layered network, the failure of SONET link BC also affects ATM demand on ATM logical link BC. Thus, ATM-level restoration also needs to be done to restore the affected ATM demand (2 VWPs). As per

Equation 5.3, this takes a restoration time of 3.3 ms.

3. Failure of logical ATM link BC

Since the ATM layer is the highest service layer of the network in consideration, only ATM services are affected by an ATM layer failure. In this case, the demand of 2 VWPs on ATM logical link BC is affected. The complete restoration of this demand, using Equation 5.3, can be calculated to take 3.3 ms.

5.2.4.2 Transport Oriented Approach

In the transport-oriented approach the restoration function is handled by the lowest layer where the failure occurs. Since failures propagate to higher layers, multiple higher layer services can be restored by a single lower layer restoration function.

1. Failure of physical link CD

As discussed before, the failure of physical link CD affects 2 ATM VWPs and 2 SONET VWPs. Thus a single physical layer restoration can restore 4 higher layer services. The restoration time can be calculated using Equation 5.1, which relates the restoration time to the degree of survivability and the average link length for WDM restoration. For a target survivability of 100 % ($s_T = 1$), we have

$$\begin{aligned} t_r^{WDM} &= 0.125 + \frac{2 \times 100}{200} + 2 \times 3 + 20 \times 1 \times 4 \\ &= 87.125 \text{ms} \end{aligned}$$

If only 50 % survivability is desired, the corresponding restoration time required is 47.125 ms.

2. Failure of SONET logical link BC

For the service-transparent network, both the service-oriented and transport-oriented approaches yield the same restoration times for SONET layer

failure. Thus, for the service-transparent network, the SONET demand that is affected is 1 VWP and the time required to recover it is 23.625 ms as calculated before. However, if we have a layered network, the Failure of SONET logical link BC also affects ATM logical link BC which is mapped on to it. Thus, the SONET recovery scheme has to restore 3 VWPs (1 having native SONET demand and 2 carrying the ATM demand for ATM logical link BC). Using Equation 5.2, the time required to restore all the affected services completely, using the transport-oriented approach can be calculated to be 43.625 ms.

3. Failure of ATM logical link BC

Since the ATM layer is the highest layer of the network being considered, there is no difference between the service-oriented and transport-oriented approaches for ATM layer failure. Similarly, there is no difference between the service-transparent and layered networks too. Thus, the failure of ATM logical link affects the demand on that link (2 VWPs). As calculated before, the time required to complete recover from this failure is 3.3 ms.

5.2.4.3 Spare Capacity Allocation Schemes

In order to protect against failure, spare capacity is allocated to the different links. Pre-determined alternate paths are established to combat link failure. These spare paths, therefore, add to the working capacity of each link. If a spare path is routed through a link, then the capacity required by the spare path needs to be added to the working demand requirement of that link. It is possible, though, that no spare path passes through a particular link. In this case, that link does not require any spare capacity. The spare paths to protect against physical link failure are shown in Table 5.7.

Similarly, physically diverse spare paths are established for the logical links

Table 5.7: Physical layer spare path assignment

Physical Link	Spare Paths
AB	AD-DC-CB
BC	BA-AD-DC
CD	CB-BA-AD
AD	AB-BC-CD

too. The ATM spare paths are shown in Table 5.8 and the SONET spare paths are shown in Table 5.9.

Table 5.8: ATM layer spare path assignment

ATM Logical Link	Spare Paths
AB	AD-DC-CB
AC	AD-DC
AD	AC-CD
BC	BA-AD-DC
CD	CA-AD

Table 5.9: SONET layer spare path assignment

SONET Logical Link	Spare Paths
AB	AD-DB
AC	AD-DC
AD	AC-CD
BC	BD-DC
BD	BA-AD
CD	CA-AD

The spare capacity to be added to any link (for complete restoration) should be sufficient to accommodate the largest working capacity of the links that are protected by it. For example, in the network being considered, the physical link BC has the highest working demand (6 VWPs). It is protected by the links AB, AD and CD (from Table 5.7). Thus, the spare capacity to be added to links AB, AD and CD should be at least 6 VWPs in order to ensure complete recovery when link BC fails. Similarly, the link BC should be assigned a spare capacity of 4 VWPs.

For the service oriented approach to survivability, each network service layer is allocated spare capacity in a manner similar to that described above. For each logical layer, spare paths are pre-established and logical links are assigned spare capacity to accommodate the spare paths.

In the transport-oriented approach to survivability, there are two ways of allocating spare capacity. These are :

1. Traditional Spare Capacity Allocation

In the traditional layered spare capacity allocation, we first allocate spare capacity to the highest layer of services being offered (i.e., in this case, the ATM layer). As per the explanation given above, if we consider ATM link AB (working demand =1 VWP), from Table 5.8, it is seen that AB needs enough spare capacity to protect ATM logical link BC (working demand = 2 VWPs). Thus the total capacity (including spare capacity) of ATM link AB should be 3 VWPs. In a layered network, this ATM link is accommodated in SONET logical link AB. Thus the total working demand of SONET logical link AB is 4 VWPs (Native SONET demand of 1 VWP and ATM demand of 3 VWPs (including ATM spare capacity)). Thus the *working* SONET demand also carries the *spare* ATM demand. Similarly, the SONET link AB also needs to carry spare capacity to protect SONET logical link BD (working demand = 1 VWP). Thus, the total capacity allocated to SONET logical link AB should be $4(\text{working}) + 1(\text{spare}) = 5\text{VWPs}$.

It is clear that the above scheme is wasteful because spare capacity is allocated to the SONET layer to protect working SONET demand, which includes *spare* ATM demand in addition to the actual working SONET demand and working ATM demand. Thus, we have a “redundant redundancy”. This problem can be avoided using the “Pre-emptive Spare Capacity” approach.

2. Pre-emptive Spare Capacity Allocation

In the pre-emptive spare capacity scheme [15], a “*common pool*” of spare resources is maintained. Thus, the ATM spare capacity and the SONET spare capacity are treated as common spare resources. In the event of ATM layer failure, the ATM restoration schemes come into play and the ATM spare resources are used for recovery. Thus, ATM logical link AB will carry a spare capacity of 2 VWPs. However this spare capacity is also shared with the SONET spare capacity. In the event of a SONET or WDM layer failure, the 2 VWPs allocated to the ATM link AB are de-allocated (or pre-empted) and used to provide spare SONET capacity. Thus, the SONET working capacity does not include spare ATM capacity, unlike the traditional approach. This means to say that the working capacity of SONET link AB is 2 (1 VWP for native SONET demand and 1 VWP for ATM logical link AB) as compared to 4 in the layered approach. Spare capacity is allocated only to protect the native SONET demand and so the total capacity of SONET link AB is $2 + 1 = 3$ VWPs.

The pre-emptive spare capacity scheme results in much greater savings in larger networks, as will be seen when we analyze the more practical, 10-node network.

The above 4 node network enables us to have an understanding of how to apply the algorithm developed to analyze survivability schemes. We shall now proceed to analyze a larger, more practical network in the next section.

5.3 Survivability Analysis of a Practical Network

5.3.1 Example Network Topology

As an example for the study of the survivability approaches and spare capacity assignment schemes described in Chapter 4, based on the framework discussed above, we consider a network topology modeled on the Advanced Technology Development Network (ATDNet)[11]. This network has 10 nodes (labeled for convenience as A through J in Figure 5.5). The physical links are labeled as 1 through 10 as shown in Figure 5.5. Each node has a SONET Add/Drop Multiplexer and a WDM Add/Drop Multiplexer. The physical connectivity is shown in Figure 5.5.

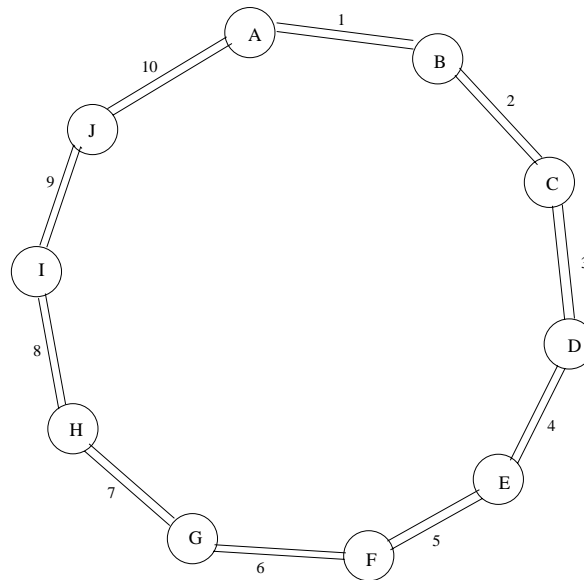


Figure 5.5: Physical topology of example network

In addition, we assume that each node except nodes E and J have ATM switches and IP routers. The logical network formed by the ATM switches is a hypercube with each node having a direct logical connection to two other nodes. This logical network is shown in Figure 5.6, with logical VP links labeled 1 through 12.

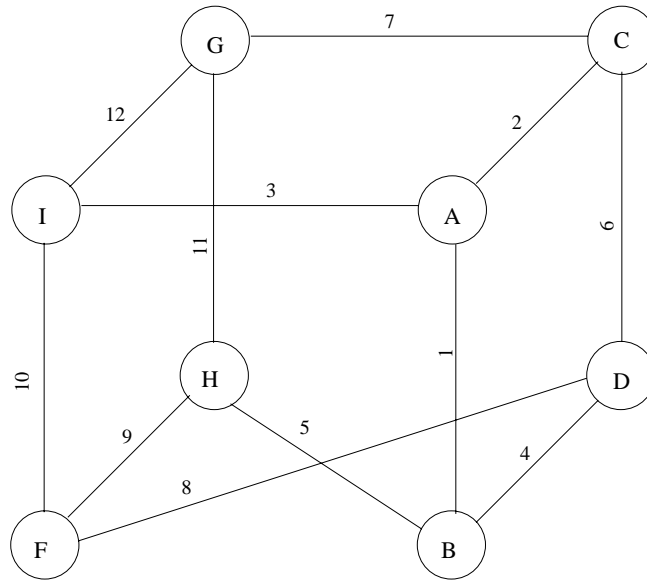


Figure 5.6: Logical ATM network topology

The physical and ATM logical connectivity is modeled on the ATDNet configuration. In addition we include a logical IP network and a Virtual Wavelength Path network.

The logical IP network shown in Figure 5.7, is also a hypercube with each node having a logical connection to three other nodes. The logical IP links (based on IP flows) are labeled 1 through 16 as shown in Figure 5.7.

The WDM layer is connected in a topology shown in Figure 5.8. This topology ensures that each node is logically connected (by means of VWPs) to at least 3 and at the most 4 other nodes. The logical links, composed of VWPs are labeled 1 through 15 as shown in Figure 5.8. In each VWP, wavelengths are assigned link-by-link, i.e., the wavelengths within a VWP have local, rather than global significance.

5.3.2 Demand Assignment

We assume a uniform demand pattern at each logical layer, i.e., all possible node pairs have equal demand, of one VWP between them. Since there are

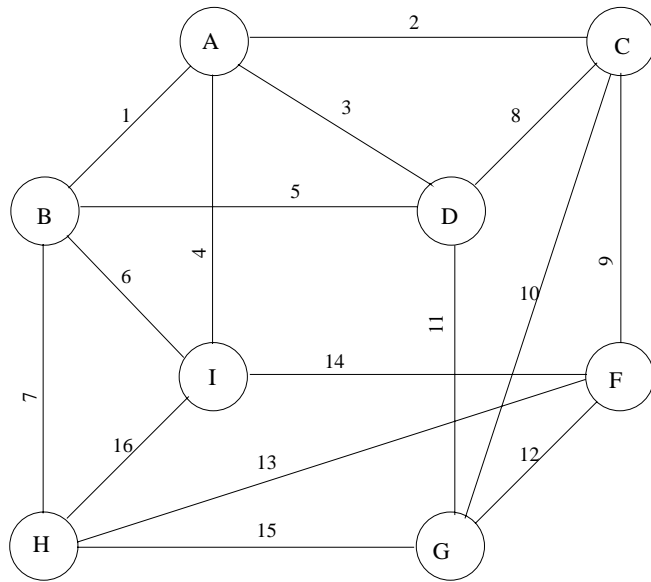


Figure 5.7: Logical IP network topology

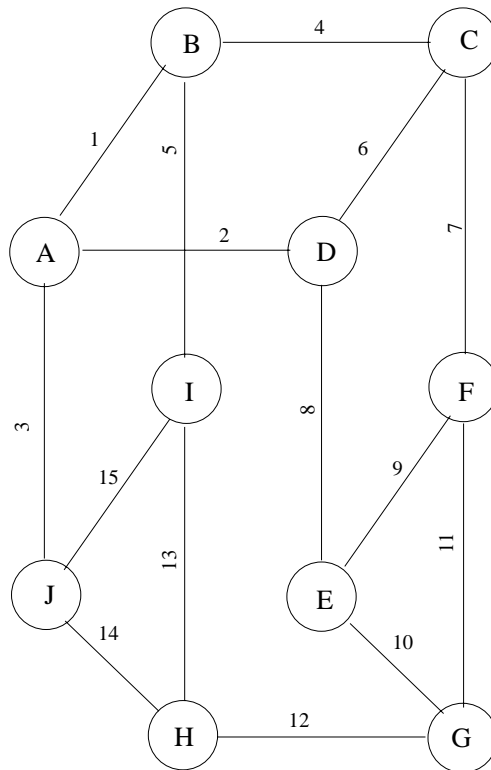


Figure 5.8: Virtual Wavelength Path Network

no point-to-point logical connections available between all node pairs (which would have been the case had we considered a fully-meshed topology), some of the demands are routed via different logical links. This demand routing is done based on the shortest-path algorithm [1]. The demand routing results in the logical links having some transit demand, in addition to the direct demand that is dropped at either node of the link. The demand requirements for each logical layer are tabulated in Tables 5.10, 5.11, 5.12.

Table 5.10: IP logical layer - demand pattern

Logical Link	Direct Demand	Transit Demand	Total Demand
AB	1	1	2
AC	1	2	3
AD	1	2	3
AI	1	2	3
BD	1	1	2
BI	1	1	2
BH	1	-	1
CD	1	1	2
CF	1	3	4
CG	1	1	2
DG	1	3	4
FG	1	-	1
FH	1	-	1
FI	1	2	3
GH	1	3	4
HI	1	2	3

The logical links are mapped on to the physical links. In the case of the transparent network, the IP, ATM and SONET demands are directly mapped to wavelength paths. In the case of the layered network, the ATM logical links carry some IP demands (due to the mapping of IP over ATM) in addition to the native ATM demand. Similarly, the SONET logical links carry some ATM demand (and consequently the IP demand carried by those ATM links) in addition to native SONET demand.

The resulting physical link demands are tabulated in Table 5.13 for the trans-

Table 5.11: ATM logical layer - demand pattern

Logical Link	Direct Demand	Transit Demand	Total Demand
AB	1	3	4
AC	1	2	3
AI	1	3	4
BD	1	3	4
BH	1	2	3
CD	1	3	4
CG	1	3	4
DF	1	4	5
FH	1	2	3
FI	1	2	3
GH	1	4	5
GI	1	1	2

Table 5.12: SONET logical layer - demand pattern

Logical Link	Direct Demand	Transit Demand	Total Demand
AB	1	6	7
AD	1	6	7
AJ	1	7	8
BC	1	7	8
BI	1	6	7
CD	1	3	4
CF	1	4	5
DE	1	7	8
EF	1	1	2
EG	1	4	5
FG	1	4	5
GH	1	7	8
HI	1	6	7
HJ	1	3	4
IJ	1	1	2

parent network.

For the layered network, the IP demands carried by the ATM logical links, along with the native ATM demands are tabulated in Table 5.14. Similarly, the ATM demands (including the IP demands) carried by the SONET logical links, along with native SONET demands are tabulated in Table 5.15. Finally, the physical links and the SONET demands carried by them are shown in Table 5.16.

5.3.3 Failure Scenarios

In order to keep our illustrative analysis simple, we consider only single link failures because these are the most commonly occurring failures. We consider the effect of single physical link failures (i.e., a fiber cut or a laser failure or any other equipment failure that renders any of the physical links shown in Figure 5.5 inaccessible to the rest of the network) and single logical link failures (i.e., failure of WDM, SONET, ATM or IP equipment or any other failure that renders any of the logical links shown in the logical topologies of Figures 5.6, 5.7 and 5.8 inaccessible to the rest of the logical network). Since any equipment failure would lead to the failure of the physical or logical links that are connected to that piece of equipment, it makes sense to treat any kind of failure in terms of link failures. We also make the realistic assumption that the Mean Time Between Failures (MTBF) is much greater than the time required to recover from a failure. This means that there is no further failure occurrence during the time when a failure is being repaired. The analysis can be extended very easily to compute the effects of multiple link failures. Node failures can be considered to have the same effect as simultaneous failure of all the links that are connected to that node. Node failures may include the failures of the WADM, the SONET ADM, the ATM switch or the IP router at a node.

Table 5.13: Physical Link Working Demands (Transparent Network)

Physical Link	SONET Links (Demand)	ATM Links (Demand)	IP Link (Demand)	Total Demand
AB	AB (7) AD (7) BI(7)	AB(4) AC(3) BH(3)	AB(2) AC(3) AD(3) BH(1) BI(2)	42
BC	BC(8) AD(7)	AC(3) BD(4)	AC(3) AD(3)	28
CD	CD(4) AD(7) CF(5)	CD(4) BD(4) CG(4)	AD(3) CG(2) CF(4)	37
DE	DE(8) CF(5)	CG(4) DF(5)	CG(2) CF(4) DG(4)	32
EF	EF(2) EG(5) CF(5)	CG(4) DF(5)	CG(2) CF(4) DG(4)	31
FG	FG(6) EG(5)	CG(4) FI(3) FH(3)	FG(1) DG(4) CG(2) FI(3) FH(1)	32
GH	GH(8)	GH(5) FH(3) FI(3)	GH(4) FH(1) FI(3)	27
HI	HI(7) HJ(4)	GI(2) BH(3) FI(3)	HI(3) BH(1) FI(3)	26
IJ	IJ(2) HJ(4) BI(7)	BH(3) AI(4)	BH(1) BI(2) AI(3)	26
JA	AJ(8) BI(7)	AI(4) BH(3)	AI(3) BI(2) BH(1)	28

Table 5.14: ATM logical Links and native ATM demands and their IP Working Demands (Layered Network)

ATM Logical Link(Native Demand)	IP Logical Links (Demand)	Total demand
AB(4)	AB(2)	6
AC(3)	AC(3) AD(3)	9
AI(4)	AI(3)	7
BD(4)	BD(2)	6
BH(3)	BI(2) BH(1)	6
CD(4)	AD(3) CD(2) CF(4) DG(4)	17
CG(4)	CG(2) DG(4)	10
DF(5)	CF(4)	9
FH(3)	FG(1) FH(1)	5
FI(3)	FI(3)	6
GH(5)	BI(2) FG(1) GH(4) HI(3)	15
GI(2)	BI(2) HI(3)	7

Table 5.15: SONET Links, their native demands and their ATM Working Demands (Layered Network)

SONET Link (Native Demand)	ATM Links (Demand)	Total Demand
AB(7)	AB(6) AC(9)	22
AD(7)	-	7
AJ(8)	AI(7)	15
BC(8)	AC(9) BD(6)	23
BI(7)	BH(6)	13
CD(4)	BD(6) CD(17)	27
CF(5)	CG(10)	15
DE(8)	DF(9)	17
EF(2)	DF(9)	11
EG(5)	-	5
FG(6)	FH(5) FI(6) CG(10)	27
GH(8)	FH(5) FI(6) GH(14) GI(2)	35
HI(7)	BH(6) FI(6) GI(5)	24
HJ(4)	-	4
IJ(2)	AI(7)	9

Table 5.16: Physical Links and their SONET Working Demands (Layered Network)

Physical Link	SONET Links (Demand)	Total Working Demand
AB	AB(22) AD(7) BI(13)	42
BC	BC(23) AD(7)	30
CD	CD(27) AD(7) CF(15)	49
DE	DE(17) CF(15)	32
EF	EF(11) EG(5) CF(15)	31
FG	FG(27) EG(5)	32
GH	GH(35)	35
HI	HI(24) HJ(4)	28
IJ	IJ(9) HJ(4) BI(13)	26
JA	AJ(15) BI(13)	28

The following failure scenarios are considered:

- All possible single physical link failures (There are 10 such possibilities as is evident from Figure 5.5). These can be considered as SONET physical link failures.
- All possible single logical link failures at the VWP layer (There are 15 such possibilities, as is evident from Figure 5.8).
- All possible single logical link failures at the ATM layer (There are 12 such possibilities, as is evident from Figure 5.6).
- All possible single logical link failures at the IP layer (There are 16 such possibilities, as is evident from Figure 5.7).

We consider first a completely service transparent network, wherein the different logical paths are directly mapped to Virtual Wavelength Paths without any intermediate layering. Next we consider a completely layered approach, where the IP logical network is mapped on to the ATM logical network, which is then mapped on to the SONET logical network which is carried on the WDM physical network.

5.3.4 Survivability Analysis with Service-Oriented Approach

As described in Chapter 4, in the Service-Oriented Approach, the survivability scheme is implemented by the highest affected network layer, irrespective of the origin of the failure. It is clear from Tables 5.13 through 5.16, that single lower-layer failures propagate to multiple higher-layer failures. In order to avoid time-consuming dynamic spare capacity assignment and rerouting, physically diverse protection paths and spare capacities to achieve a target survivability s_T are pre-allocated.

5.3.4.1 Failure at WDM level

Since this is the lowest layer, all the higher layer services will be affected. Thus, each of the higher layers perform their own restoration schemes.

1. Transparent Network

From Table 5.13, for a single physical link failure, say link AB, the number of SONET logical links to be restored is 3 (AB, AD and BI). The number of ATM restorations to be carried out is also 3 (AB, AC and BH). The IP restoration amounts to 5 logical IP links (AB, AC, AD, BH and BI).

The total demand to be restored by each service layer can be obtained from Table 5.13. The restoration times for the different restoration schemes can be obtained from Equations 5.1 through 5.4. We consider three different geographical sizes of networks - One with average link length = 10 km, which is more like a Local Area Network, one with average link length = 300 km, which represents a Metropolitan Area Network and the third, which represents a Wide Area Network with average link length = 1000 km.

- **Restoration of native SONET demand.**

For a single link failure at the WDM layer, multiple SONET demands have to be restored. For the example network, SONET restoration[1] is applied. The degree of survivability $s(t_r)$ is plotted as a function of average restoration time for the three different network sizes. The function $s(t_r)$ can be easily obtained using Equation 5.2 (which relates t_r^{SONET} with the degree of survivability s). This is shown in Figure 5.9.

- **Restoration of native ATM demand.**

Native ATM demand is restored using the fast VP restoration scheme described in [8]. The survivability degree versus average restoration

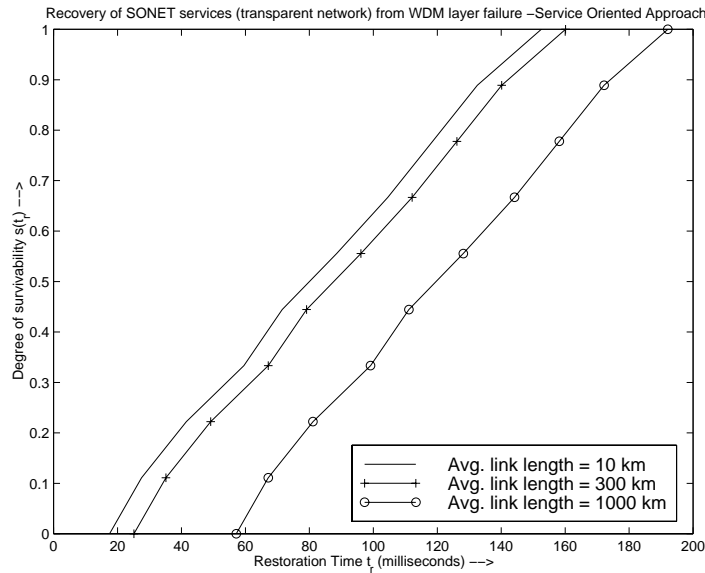


Figure 5.9: Degree of Survivability as a Function of Restoration Time for SONET protection against WDM layer failures (Service-Oriented Approach, Transparent Network)

time is plotted in Figure 5.10. As expected, and as already shown in the illustrative example of Section 5.2 the ATM restoration scheme is much faster than SONET. Also, since the ATM restoration time per VP is really fast (see the last term of Equation 5.3), the time difference between zero survivability and complete restoration is very small, as a result of which the curve has a very steep slope. The advantage in restoration speed of the ATM restoration scheme is clearly evident from the figure.

- **Restoration of native IP demand.**

IP demand can be rerouted using the scheme described in [12]. The degree of survivability versus average restoration time is plotted in Figure 5.11. As suggested by Equation 5.4, the IP restoration scheme is the slowest of all the four layers being considered. This is evident in the curve shown in Figure 5.11.

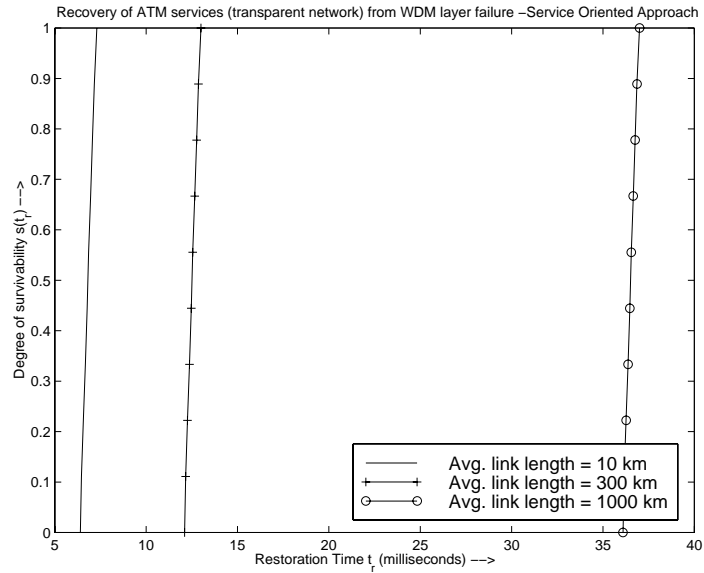


Figure 5.10: Degree of Survivability as a Function of Restoration Time for ATM protection against WDM layer failures (Service-Oriented Approach, Transparent Network)

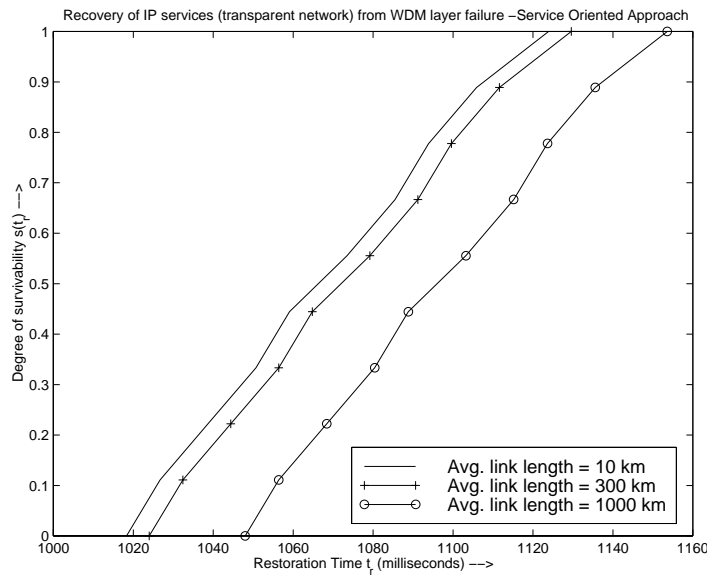


Figure 5.11: Degree of Survivability as a Function of Restoration Time for IP protection against WDM layer failures (Service-Oriented Approach, Transparent Network)

2. Layered Network

- **Restoration of native SONET demand.**

The degree of survivability $s(t_r)$ is plotted as a function of average restoration time for SONET service restoration in the layered network, in the event of a failure at the WDM layer. This is shown in Figure 5.12.

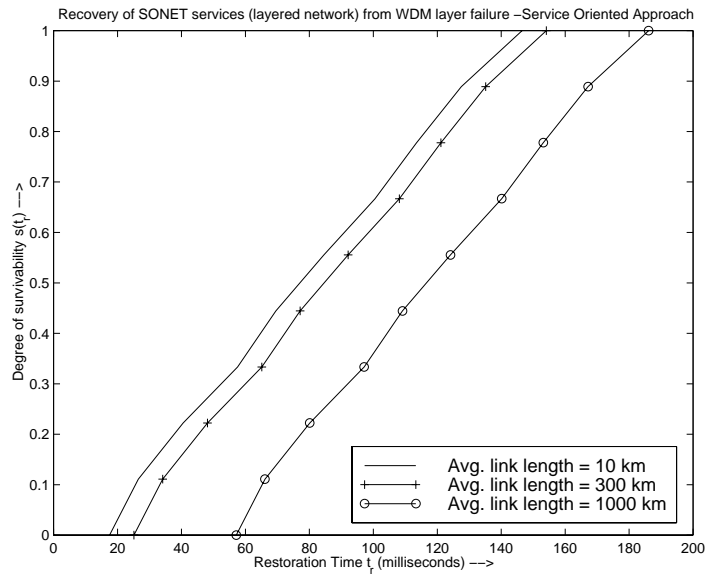


Figure 5.12: Degree of Survivability as a Function of Restoration Time for SONET protection against WDM layer failures (Service-Oriented Approach, Layered Network)

- **Restoration of native ATM demand.**

The survivability degree for ATM restoration in the event of WDM layer failure, versus average restoration time is plotted in Figure 5.13.

- **Restoration of native IP demand.**

The degree of survivability for IP services against WDM layer failure, versus average restoration time is plotted in Figure 5.14.

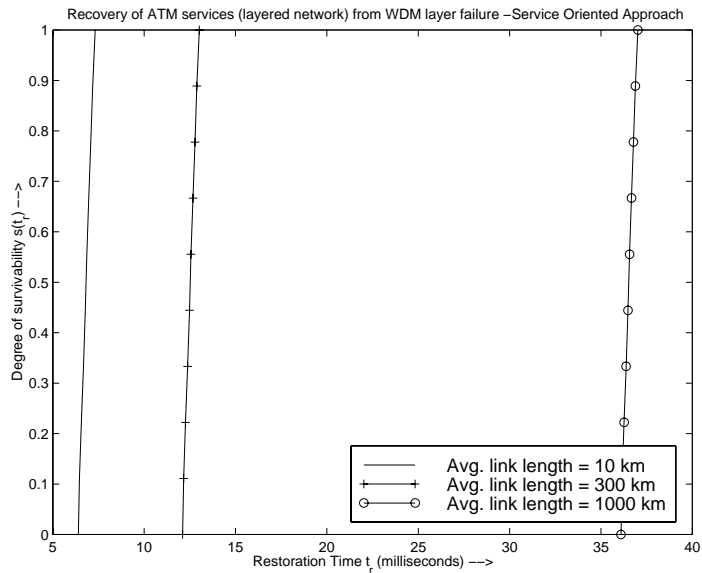


Figure 5.13: Degree of Survivability as a Function of Restoration Time for ATM protection against WDM layer failures (Service-Oriented Approach, Layered Network)

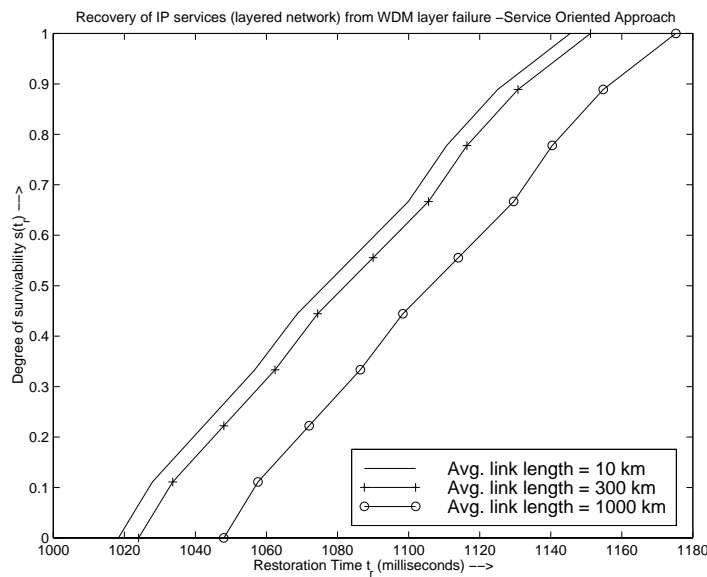


Figure 5.14: Degree of Survivability as a Function of Restoration Time for IP protection against WDM layer failures (Service-Oriented Approach, Layered Network)

5.3.4.2 Failure at the SONET layer

1. Transparent Network

In the transparent network, SONET demand is mapped directly on to the WDM layer. Thus, a SONET layer failure affects only the native SONET demand and no other service is affected.

- **Restoration of native SONET demand.**

The degree of survivability for recovery from SONET failure is plotted against the average restoration time in Figure 5.15. The sudden jump from $s = 0$ to $s = 0.1$ that is observed in the curve is a result of truncation of restored demand to the nearest integer value, before substituting it in Equation 5.2. For example, if the affected demand is equal to 4 VWPs, then if $s = 0$, the number of VWPs restored is 0. If $s = 0.1$ then the number of VWPs restored is $0.1 \times 4 = 0.4$. Since the number of VWPs is an integer, the above value is truncated to 0. The effect of this truncation (or quantization, since s is not a continuous function of t_r) is seen in the form of discontinuities in the curve, like the jump from $s = 0$ to $s = 0.1$. It should be noted that the behaviour of the curve for low values of s is really not of much interest, as we are concerned about the time taken to restore services to a sufficiently high percentage (if not 100 %) of the affected services.

2. Layered Network

In the layered network, a failure at the SONET layer leads to loss of native SONET demand on the logical link that failed, as well as multiple losses of ATM demand (and the IP demand mapped on to the logical ATM links that are affected). Therefore, the service-oriented approach involves recovery at the SONET layer, ATM layer as well as at the IP layer.

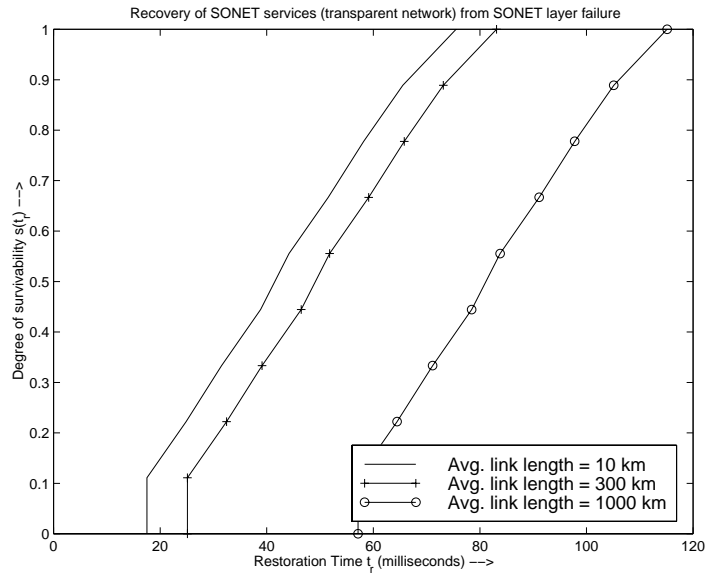


Figure 5.15: Degree of Survivability as a Function of Restoration Time for SONET protection against SONET layer failures (Service-Oriented Approach, Transparent Network)

- **Restoration of native SONET demand.**

The degree of survivability for SONET restoration, in the event of a SONET layer failure, versus the average restoration time is shown in Figure 5.16.

- **Restoration of native ATM demand.**

In Figure 5.17, we show the degree of survivability of ATM restoration against single SONET link failure, for a layered network, as a function of the average restoration time.

- **Restoration of native IP demand.**

The IP demand that is affected by a failure in the SONET layer, is restored using the IP restoration scheme discussed in [12]. The degree of survivability as a function of average restoration time is shown in Figure 5.18

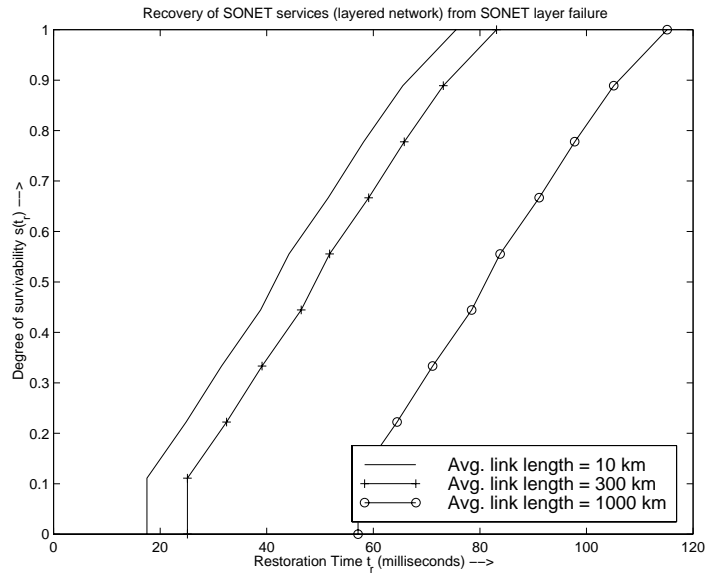


Figure 5.16: Degree of Survivability as a Function of Restoration Time for SNET protection against SNET layer failures (Service-Oriented Approach, Layered Network)

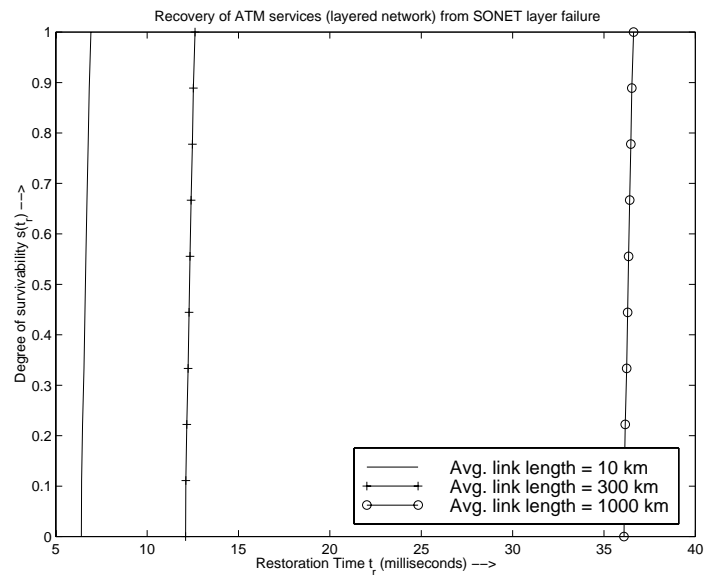


Figure 5.17: Degree of Survivability as a Function of Restoration Time for ATM protection against SNET layer failures (Service-Oriented Approach, Layered Network)

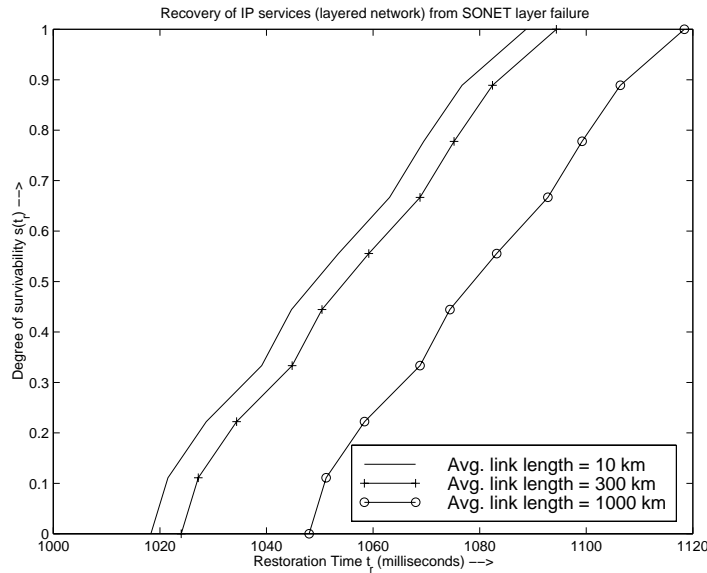


Figure 5.18: Degree of Survivability as a Function of Restoration Time for IP protection against SONET layer failures (Service-Oriented Approach, Layered Network)

5.3.4.3 Failure at the ATM layer

1. Transparent Network

In the transparent network, since demands are directly mapped on to the WDM layer, an ATM layer failure will affect only the native ATM demand.

- **Restoration of native ATM demand.**

The degree of survivability for ATM demand restoration, in the event of a failure at the ATM layer itself, for a transparent network is plotted against the average restoration time. This is shown in Figure 5.19. Again, it can be noted that due to extremely fast restoration of ATM VP's, the slope of the curve is very steep.

2. Layered Network

In the layered network, a failure at the ATM layer affects the native ATM

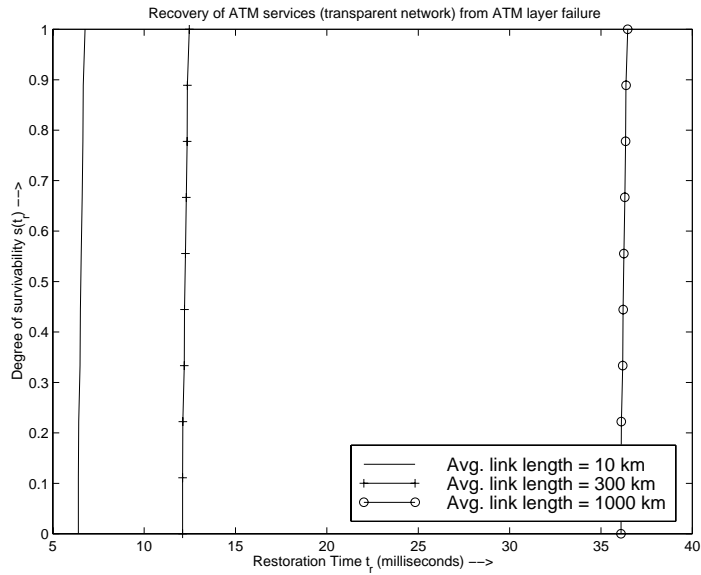


Figure 5.19: Degree of Survivability as a Function of Restoration Time for ATM protection against ATM layer failures (Service-Oriented Approach, Transparent Network)

demand as well as the higher layer IP demand that is mapped on to the affected logical ATM link. Hence, separate recovery procedures at the ATM and IP layers are necessary to recover the affected demand, using the Service-Oriented Approach.

- **Restoration of native ATM demand.**

In Figure 5.20, we show the degree of survivability as a function of average restoration time for native ATM demand restoration after a failure at the ATM layer itself.

- **Restoration of native IP demand.**

Figure 5.21 shows the degree of survivability for IP demand recovery after an ATM layer failure, versus the average restoration time.

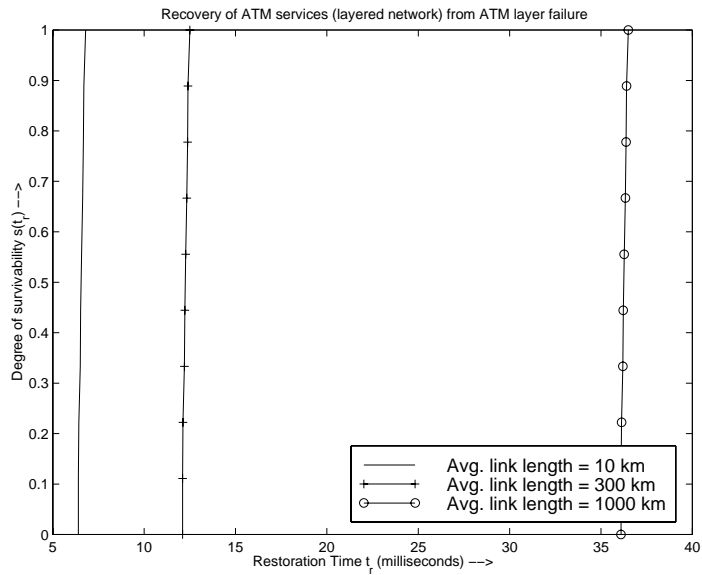


Figure 5.20: Degree of Survivability as a Function of Restoration Time for ATM protection against ATM layer failures (Service-Oriented Approach, Layered Network)

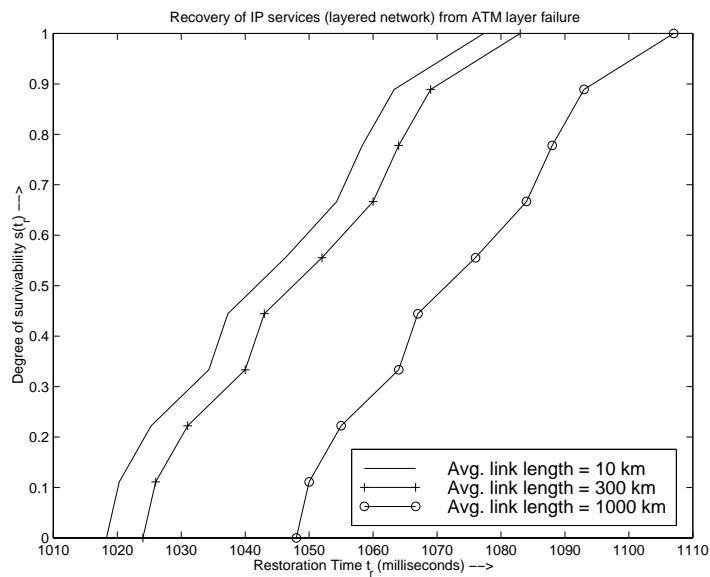


Figure 5.21: Degree of Survivability as a Function of Restoration Time for IP protection against ATM layer failures (Service-Oriented Approach, Layered Network)

5.3.4.4 Failure at the IP layer

Since IP is the highest layer in the layered-network case, the effect of network layering is not seen in the IP restoration schemes. Consequently, both the service-oriented and transport-oriented approaches have the same effect for restoration against failures at the IP layer. The degree of survivability for IP restoration against IP layer failure, is plotted versus the average restoration time in Figure 5.22. It should be noted that fewer services are affected at the IP layer due to failure at that layer itself, as compared to the number of services affected at the IP layer due to failure at a lower layer. This is because, the lower layer logical links carry multiple IP demands. Since the number of services to be restored is less, the time for complete restoration is also the least as compared to the IP restoration time due to lower layer failures. Also, since the number of services to be restored is less, the effect of truncation (s times the affected demand is rounded off to the nearest integer value as it represents the demand to be restored) is more pronounced in the nature of the curve, as a result the curve in Figure 5.22 is not as smooth as the other curves for IP restoration.

5.3.5 Survivability Analysis with Transport-Oriented Approach

In the transport-oriented approach, as discussed in Chapter 4, the lowest layer that causes the failure, is responsible for performing the restoration function. Thus, multiple higher layer services are restored by a single lower layer restoration function.

It should be noted that, in the case of the transparent network, the transport-oriented approach is different from the service-oriented approach only in the event of physical layer failure. Since the higher-layer services are directly mapped on to the WDM layer, any higher layer failure restoration using the Transport-Oriented approach is exactly the same as the Service-Oriented approach dis-

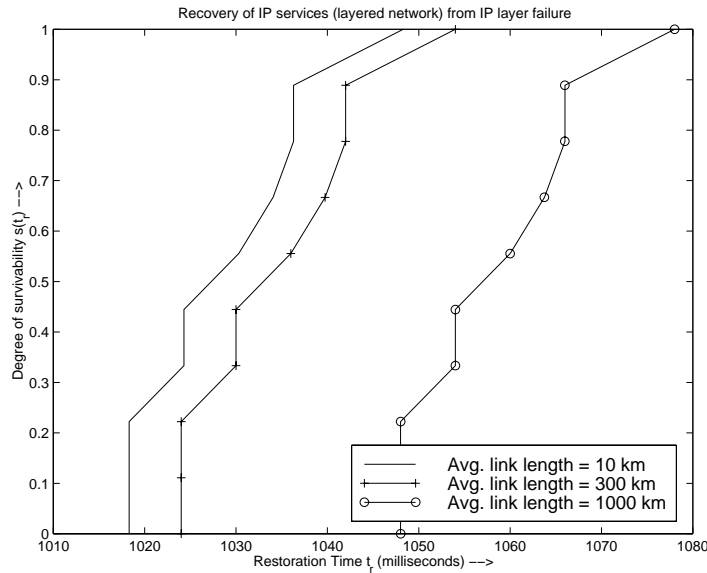


Figure 5.22: Degree of Survivability as a Function of Restoration Time for IP protection against IP layer failures

cussed in the previous section.

5.3.5.1 Failure at the WDM Layer

In the case of a WDM layer failure, the recovery at the WDM layer itself restores all the affected demand at the higher layers, provided enough spare capacity is provided to attain the desired target survivability s_T .

1. Transparent Network

The total number of services that are affected by a single WDM layer failure, for the transparent network, is obtained from Table 5.13. The degree of survivability versus the average restoration time, for WDM failure recovery using the Transport-Oriented approach is plotted in Figure 5.23. As seen in the figure, the non-linear effects of truncation are not easily visible and the curves appear more linear. This is because of the increased number of VWPs affected at the WDM layer as compared to higher layers, as seen from Table 5.13.

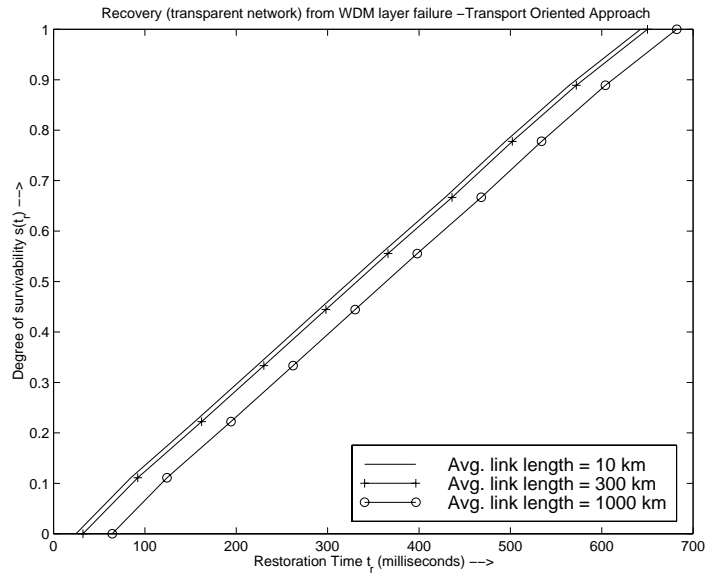


Figure 5.23: Degree of Survivability as a Function of Restoration Time for protection against WDM layer failures -Transparent Network, Transport-Oriented Approach

2. Layered Network

The total number of services affected in the layered network, due to single WDM layer failures, is obtained from Table 5.16

The degree of survivability to restore the affected services, is plotted versus the restoration time, in Figure 5.24.

5.3.5.2 Failure at the SONET Layer

The effect of SONET layer failure, and recovery at the SONET layer itself on the degree of survivability and restoration time is studied for the Layered Network. For the transparent network, the effect will be the same as the service-oriented approach, as explained earlier. Hence, we study only the effect of SONET layer recovery in the Layered network.

Native SONET, ATM and IP services can be restored by performing restoration at the SONET layer itself. The degree of survivability for this case is plotted

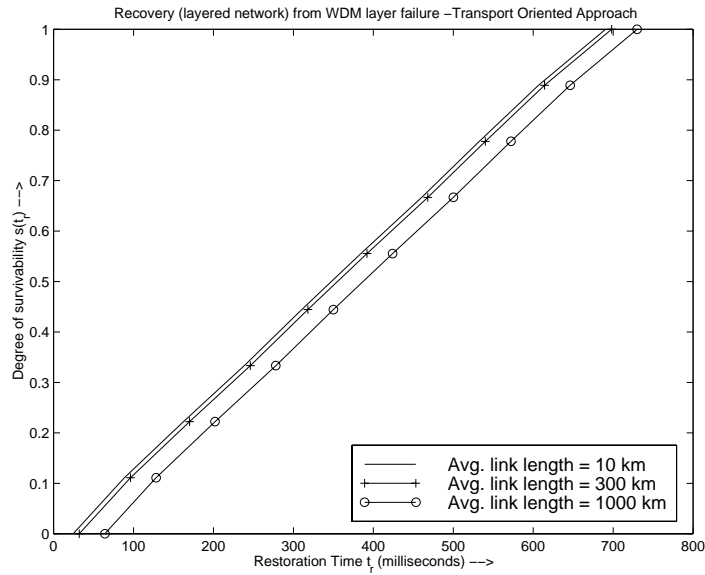


Figure 5.24: Degree of Survivability as a Function of Restoration Time for protection against WDM layer failures -Layered Network, Transport-Oriented Approach

against the average restoration time in Figure 5.25.

5.3.5.3 Failure at the ATM Layer

Only the impact of ATM layer failure on the layered network is studied, based on the argument supplied before. The native ATM demand as well as the IP demand that is carried on the ATM links are recovered using ATM restoration. The degree of survivability versus restoration time is plotted in Figure 5.26.

5.3.5.4 Failure at the IP Layer

As discussed before, this case is the same as the service-oriented case (for both transparent and layered networks). This is because IP is the highest layer in the layered network.

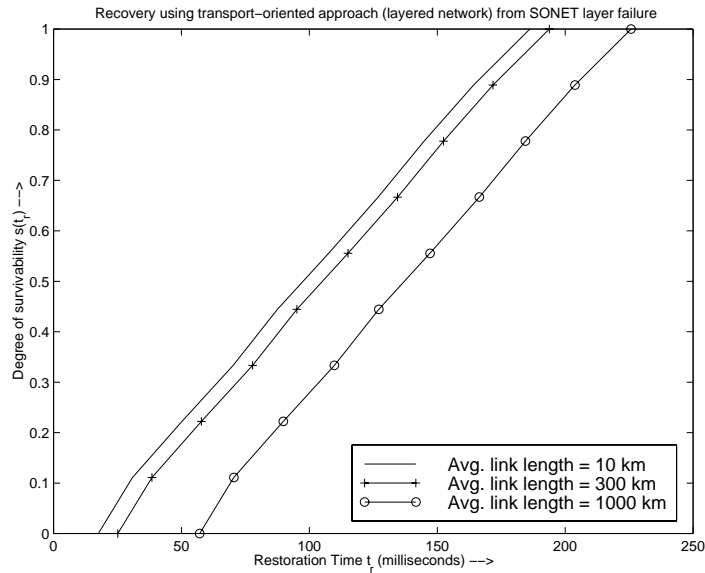


Figure 5.25: Degree of Survivability as a Function of Restoration Time for protection against SONET layer failures -Layered Network, Transport-Oriented Approach

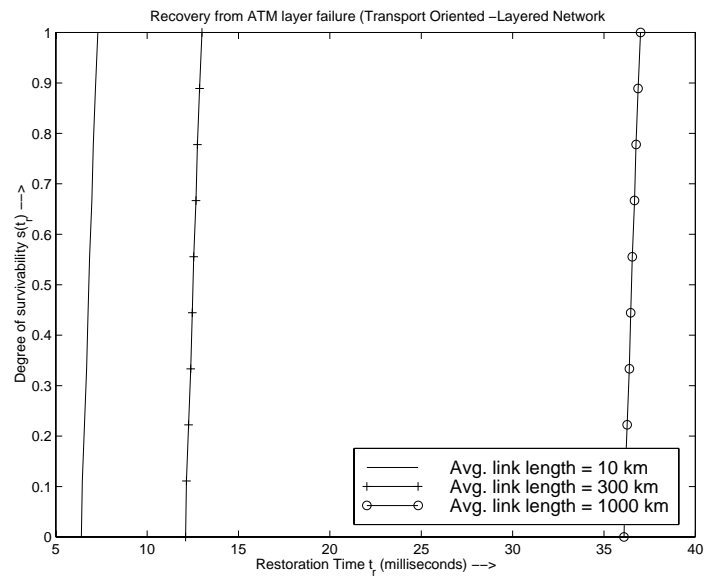


Figure 5.26: Degree of Survivability as a Function of Restoration Time for protection against ATM layer failures -Layered Network, Transport-Oriented Approach

5.3.6 Spare Capacity Allocation

In order to ensure 100 % survivability, the spare routes for each failure (physical as well as logical link) must be designed to be on physically diverse paths. Extra capacity needs to be allocated to each link so as to accommodate spare paths for all possible link failures. It is possible that a particular link does not carry any spare paths, as none of the spare routes for the rest of the links include that particular link. As a result of this, there may be certain links that have zero spare capacity, as will be seen in the sections to follow. It should be noted that this **does not mean** that the particular link is unprotected, it only means that that link **does not protect** any other links.

5.3.6.1 Spare Capacity Allocation for Service-Oriented Approach

In the service-oriented approach, the affected working demands of each of the network service layers (SONET, ATM and IP) need to be restored. Thus, spare capacity needs to be allocated separately to each of the logical links of each network layer. The spare capacity assignments for the different network layers for the service-oriented approach, are made in order to ensure 100 % survivability, and physically diverse spare paths. The diverse spare paths can be obtained using well known algorithms [1]. These spare capacities are shown in Tables 5.17, 5.18 and 5.19.

5.3.6.2 Traditional Layered Spare Capacity Allocation for Transport-Oriented Approach

In the Transport-Oriented Approach, with the traditional spare capacity allocation, we first allocate spare capacity to obtain the desired survivability degree at the highest layer (i.e., the IP layer). The layer below (i.e., the ATM layer) has to have a working capacity which is equal to the sum of the native working ATM demand and the transported IP working demand *as well as* the spare IP

Table 5.17: SONET layer spare capacity assignment

SONET Logical Link	Working Demand	Spare Capacity	Total Demand
AB	7	8	15
AD	7	8	15
AJ	8	8	16
BC	8	8	16
BI	7	6	13
CD	4	7	11
CF	5	8	13
DE	8	8	16
EF	2	0	2
EG	5	8	13
FG	6	8	14
GH	8	8	16
HI	7	8	15
HJ	4	8	12
IJ	2	0	2

Table 5.18: ATM layer spare capacity assignment

ATM Logical Link	Working Demand	Spare Capacity	Total Demand
AB	4	0	4
AC	3	5	8
AI	4	5	9
BD	4	5	9
BH	3	5	8
CD	4	5	9
CG	4	5	9
DF	5	4	9
FH	3	4	7
FI	3	5	8
GH	5	4	9
GI	2	4	6

Table 5.19: IP layer spare capacity assignment

IP Logical Link	Working Demand	Spare Capacity	Total Demand
AB	2	2	4
AC	3	4	7
AD	3	0	3
AI	3	4	7
BD	2	4	6
BH	2	4	6
BI	1	3	4
CD	2	0	2
CF	4	3	7
CG	2	0	2
DG	4	4	8
FG	1	0	1
FH	1	0	1
FI	3	4	7
GH	4	4	8
HI	3	3	6

demand. Similarly, the SONET layer has to accommodate the working native SONET demand, as well as the working *and* spare ATM demand (which also includes working and spare IP demand). It is clear, therefore, that the lower layer spare capacity needs to be assigned to protect the higher layer working and spare capacity, in addition to the working native capacity. This “redundant redundancy” is clearly wasteful. This is evident from Table 5.20, which shows the spare capacity requirement for achieving 100 % survivability. An example of how the spare capacity is calculated using the layered approach is discussed in Section 5.2.4.3 for the 4-node example network.

5.3.6.3 Pre-emptive Spare Capacity Allocation for Transport-Oriented Approach

In this approach, a “common pool” of spare resources is kept for use by any of the network layers. In the case of a failure at a lower layer, the spare resources being used by the higher layer are pre-empted, as described in Chapter 4. It is

Table 5.20: Traditional layered spare capacity assignment

Physical Link	Working Demand (original)	Working Demand (including spare for higher layers)	Spare Capacity	Total Demand
AB	42	103	239	342
BC	30	86	160	246
CD	49	136	262	398
DE	32	87	218	305
EF	31	86	218	304
FG	32	89	218	307
GH	35	116	102	218
HI	28	106	195	301
IJ	26	85	195	280
JA	28	88	195	283

highly advantageous to use this scheme, as it reduces the capacity requirement to a large extent. The spare capacity required for each physical link, using the pre-emptive allocation scheme, is shown in Table 5.21

Table 5.21: Pre-emptive spare capacity assignment

Physical Link	Working Demand	Spare Capacity	Total Demand
AB	42	75	117
BC	30	52	82
CD	49	76	125
DE	32	62	94
EF	31	62	93
FG	32	62	94
GH	35	27	62
HI	28	58	86
IJ	26	58	84
JA	28	58	86

Finally, for the service transparent network, the spare capacity assignment for each of the services is similar to the assignment shown for the service-oriented approach in Tables 5.17, 5.18 and 5.19. Using the mappings of these services on to the physical links, the total spare capacity requirements for the physical links can be calculated. A comparison of the total capacity require-

ment (with and without spare capacity) for the two spare capacity allocation schemes for a layered network, and the spare capacity requirement for a service-transparent network is shown in Table 5.22. The same comparison is also depicted graphically in Figure 5.27, where the results of Table 5.22 are shown relative to a working link capacity of 1 unit.

Table 5.22: Comparison of link capacity requirements

Physical Link	Without Spare Capacity	Using Layered Approach	Using Preemptive Approach	Service-Transparent Network
AB	42	342	117	87
BC	30	246	82	58
CD	49	398	125	78
DE	32	305	94	64
EF	31	304	93	63
FG	32	307	94	70
GH	35	218	62	56
HI	28	301	86	68
IJ	26	280	84	61
JA	28	283	86	63

It is clear that the common-pool scheme, if implemented, results in a much lower cost network (since network cost is directly related to the capacity requirement) when we have a layered network architecture. However, the spare capacity requirements of the service-transparent network are even lower. This is a significant advantage of service transparency.

5.4 Recommendations based on Performance Evaluation of Different Survivability Approaches

Based on the results observed in the previous section, the following observations can be made:

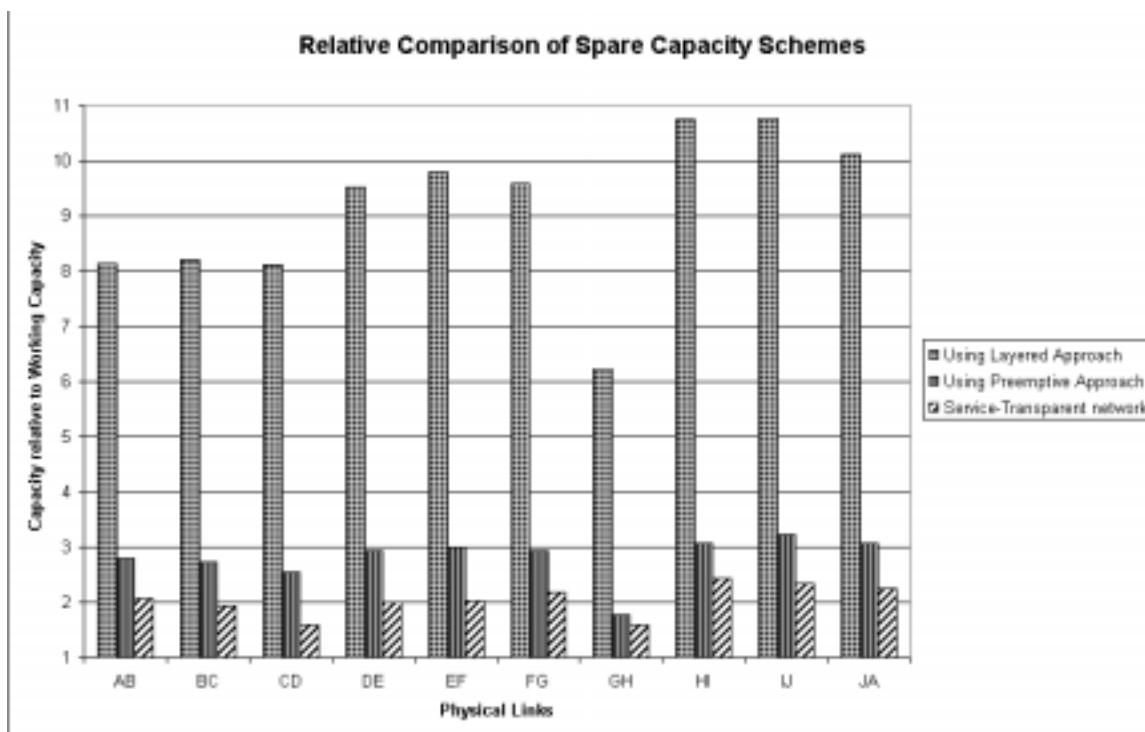


Figure 5.27: Comparison of Spare Capacity schemes

5.4.1 Service Oriented versus Transport Oriented

1. Service-Oriented survivability approach

- If the failure occurs at the WDM layer, then all the services that are affected have to perform their respective restoration action. This is observed to be time-consuming since multiple restoration actions have to be performed, for each kind of service.
- In the case of a service-transparent network, if the failure occurs at the SONET layer, then only SONET services need to be restored. No other services need to be restored as they are not affected by SONET layer failure. Also, since fewer SONET services are affected by a SONET layer failure, as compared to a WDM layer failure, the restoration time for SONET services due to SONET layer failure is also less than that due to a WDM layer failure.

A similar argument holds true for each type of service, i.e., as the failure occurs at the service layer, the number of services to be restored decreases, leading to faster restoration.

- In the case of a layered network, SONET layer failures lead to loss of service at the ATM and IP layers too, as these services are mapped on to the SONET layer. Thus, multiple restoration actions need to be performed, just like in the case of a WDM layer failure. Similarly, ATM layer failures lead to failures in the IP layer too.
- It is clear that the number of restoration functions to be performed using the Service-Oriented Approach, is the least when the failure occurs at the service layer itself. Thus, the service-oriented approach is recommended when it is highly likely that a failure occurs at that layer. Otherwise, it involves a lot of restoration actions being taken.
- The service-oriented approach is most unsuitable for the IP layer as IP layer restoration is extremely slow.

2. Transport-Oriented Survivability Approach

- In the transport oriented approach, multiple higher layer services are restored when the layer where the failure occurs is restored. Thus, WDM restoration is used to restore services affected by a failure at the WDM layer. In the example network that we consider, it is seen that WDM restoration is slower than SONET or ATM restoration, but much faster than IP restoration. This might not be generally true. If the demand distribution of the network is such that the demand to be restored at the higher layers is considerable, then the SONET layer restoration may be slower than the WDM layer restoration. However, ATM restoration is at a clear advantage because it is extremely fast as compared to the other restoration mechanisms.

- It is also observed that in a layered network, the transport-oriented restoration due to a failure at the SONET layer, is slower than the service-oriented restoration due to a failure at the SONET layer. This is because, in the former case, the ATM demand mapped on to the SONET layer also forms a part of the SONET demand to be restored, as opposed to only the native SONET demand being restored in the service-oriented approach. This difference is not easily discernible in the case of an ATM layer failure because the ATM restoration is inherently fast. Similarly, this difference in the restoration times between the service-oriented and transport-oriented approaches is not discernible in the case of a service-transparent network.
- The IP layer is clearly benefits (except, of course, if the failure occurs at the IP layer itself) in the Transport-Oriented approach, as any of the lower layer schemes is much faster than IP restoration.

5.4.2 Service-Transparent versus Layered Network

1. In a service-transparent network, different services are directly mapped on to the physical layer. This, coupled with the service-oriented approach to survivability, ensures that a single survivability scheme is responsible for restoring a particular service. Thus, in a transparent network, with the service-oriented approach, all ATM services will be restored by ATM restoration mechanisms only. This is an added advantage if the restoration scheme is fast (as is the ATM restoration scheme), and the most likely failures occur at the service layer itself. On the other hand, multiple survivability schemes must co-exist in a layered network.
2. The direct mapping of services on to the physical network leads to reduced demand requirement, and therefore, reduced network costs. An-

other general observation, not studied in this work, is that service transparency also avoids the overhead of encapsulating different service formats in intermediate layers and maximizes the transport of “useful” information, rather than wasting bandwidth using multiple headers and trailers.

5.4.2.1 Layered Spare Capacity Allocation versus Pre-emptive Spare Capacity Allocation

1. The advantage of using the pre-emptive spare capacity scheme for spare capacity allocation has been observed in the analysis of our example network.
2. The advantage of the traditional layered spare capacity allocation is its simplicity. The complexity involved in maintaining a “common-pool” of spare resources results from the need to translate the varying spare capacity requirements of the different layers into a common unit. We have shown that multiwavelength optical networks enable us to translate the capacity requirements of the different layers in terms of VWPs. Thus, the use of the pre-emptive scheme is now realistic.

In addition to the above, it was also observed that propagation delays form a major part of the restoration times, especially when the average link lengths are large (1000 km and above).

It should be noted that the observations made in the analysis are more or less general and are not confined to the example network being considered. Thus, the algorithm can be applied quite generally to any kind of network to evaluate any kind of survivability scheme and spare capacity allocation scheme. Finally, the main findings of our analysis are summarized in Table 5.23.

Table 5.23: Main Findings of our analysis

Feature	Finding	Recommendation
Service Oriented Scheme	Multiple higher layer restorations for single lower layer failure	Good for Service-transparent networks, where failure occurs at service layer
Transport Oriented Scheme	Single lower layer restoration restores multiple higher layer services	Good for Layered networks where lower layer failures are more common
Service-transparent networks	Reduce capacity requirements and network overhead	Recommended for future high-speed optical networks
ATM VP restoration	extremely fast	Use as far as possible (irrespective of service transparency, and survivability approach)
IP restoration	extremely slow	use only for IP layer failures
Pre-emptive spare capacity allocation	Reduces capacity requirements and network cost	Recommended for future high-speed optical networks

It should be noted that the analysis performed in this chapter is for a simple, regular network topology and for single link failures. Many simplifying assumptions regarding the processing and propagation of failure messages and the mapping of services on to VWPs has been made to simplify the analysis. More realistic analysis would require computer-based tools. This algorithm is very general and can be extended to analyze realistic networks, without the assumptions we make here.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

In this research, a general algorithm to determine the performance of different survivability architectures is proposed. The performance evaluation is based on restoration time and spare capacity required to attain a desired level of survivability. The level of survivability is determined quantitatively in terms of the degree of survivability, which is defined as the ratio of demand restored to demand affected by a failure.

The survivability requirements of different network layers - IP, ATM, SONET and WDM in particular - were summarized, and the most appropriate and popular restoration scheme for each network service were incorporated in our analysis.

An example network with ten nodes was considered for the study. Logical topologies for the different network services were assumed. The impact of the Service-Oriented and Transport-Oriented approaches on the restoration time and spare capacity requirements of the network were studied. Two different Spare capacity schemes - the traditional layered spare capacity allocation and the pre-emptive or common-pool spare capacity allocation - were com-

pared. Recommendations were made based on our findings.

6.2 Future Work

The impact of multiple link failures on the restoration time needs to be studied. The effect of IP restoration (which is still in its early stages of research) that has been discussed in this research, and its impact on future multi-service networks needs to be studied.

Since the most frequently occurring failures are single link failures, adequate protection against these failures is usually provided by pre-assigning spare capacity and alternate, physically diverse routes. The spare capacity is usually allocated to guarantee 100 % survivability against single link failures. It would be interesting to see the degree of survivability that is attainable in the event of multiple (at least double) link failures after pre-allocating spare capacity to account for single failures. In most cases, the survivability attained will not be 100 %.

In this research we have considered, for the sake of comparison, that every logical link path (a SONET path, an ATM VP or an IP flow) is mapped on to a single VWP. We have expressed demand in terms of VWPs. However, in a practical situation, the capacity requirements of say, a SONET path and an ATM VP would vary. Also, multiple logical paths may be mapped on to a single VWP. For example, it is possible that multiple ATM VPs are mapped on to a single VWP. Since the ATM restoration scheme is very fast, using a single VP over a single VWP appears to bias the results of our research heavily in favor of ATM. A more practical mapping of the logical network paths to VWPs is, therefore, an important part of future work.

Node failures can be treated as failures of all the links connected to the failed node. If the spare capacity assignment is made to account for node failures,

the network becomes 100 % survivable to all failures. Suitable topologies to minimize the spare capacity requirements need to be investigated for the node failures.

In a multi-service network some services are more critical than others. In the event of an outage, when all services on the network are equally affected, a priority-based scheme to restore the more critical services before restoring the other services, is usually used. The impact of such a scheme on restoration times and spare capacity requirements needs to be studied.

The restoration schemes discussed in this work are mostly connection based, i.e., schemes to restore failed connections. It would be interesting to see the impact of load directed restoration [29] (where the offered load for each demand pair at the time of failure is considered) for the restoration of a bundle of circuits, on the restoration time and spare capacity requirements, using the service oriented and transport oriented approaches. This idea is motivated by the offered load variation that occurs in the traffic network depending on the time of the day and taking into account dynamic all routing in the traffic network. The idea behind the load directed model is to make better use of the available reconnection capacity depending on the time of the failure. A network operations system for efficiently deciding which survivability schemes to use for what kind of failure, based on the recommendations made in our analysis, can be designed in the future. This would involve a hybrid architecture that combines the service-oriented and transport-oriented restoration schemes, and uses whichever is appropriate for the given network.

Finally, and most importantly, the validity of the algorithm to evaluate the survivability performance of different approaches needs to be tested in a real-life environment, by simulation or other techniques. Some of the assumptions made to simplify this analysis may be relaxed. Computer-based tools may be developed to compare the survivability approaches and spare capacity schemes

for a more complex network, with multiple failures and with a better mapping of services to VWPs. This analysis should be treated as the first step towards a complete understanding and design of efficient integrated survivability architectures for multi-service optical networks.

Bibliography

- [1] T. Wu, "*Fiber Network Service Survivability*," Artech House : Boston/London, 1992.
- [2] "A *Technical Report on Network Survivability Performance*," Prepared by T1A1.2, Working Group on Network Survivability Performance, Report No. 24, November 1993.
- [3] K. Sato, "*Advances in Transport Network Technologies : Photonic Networks, ATM and SDH*," London: Artech House, 1996.
- [4] S. C. Liew and K. W. Lu, "A *Framework for Characterizing Disaster-Based Network Survivability*," IEEE Journal on Selected Areas in Communications, Vol. 12, No. 1, January 1994.
- [5] O. Gerstel, R. Ramaswami and G.H. Sasaki, "*Fault-tolerant multiwavelength optical networks with limited wavelength conversion*," IEEE INFOCOM 1997.
- [6] M. R. Wilson, "*The Quantitative Impact of Survivable Network Architectures on Service Availability*," IEEE Communications Magazine, May 1998.
- [7] R. Kawamura, K. Sato, I. Tokizawa, "*Self-Healing ATM Networks Based on Virtual Path Concept*," IEEE Journal on Selected Areas in Communications, Vol. 12, No. 1, January 1994.

- [8] J. Anderson, B. T. Doshi, S. Dravida, P. Harshavardhana, "*Fast Restoration of ATM networks*," IEEE Journal on Selected Areas in Communications, Vol. 12, No. 1, January 1994.
- [9] 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.
- [10] "*Multiwavelength Optical NETWORKing*,"
<http://www.bell-labs.com/project/MONET>
- [11] "*The Bell Atlantic ATDNet Node*," <http://www.bell-atl.atd.net>
- [12] "*Using HSRP for Fault-Tolerant Using HSRP for Fault-Tolerant IP Routing*"
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icshsrp.htm>
- [13] "*Design and Evaluation Tools*," The Broadband communication networks group, Department of Information Technology. University of Ghent, Belgium,
<http://www.intec.rug.ac.be/Research/Groups/ibcn/welcome.html>.
- [14] P. Demeester, M. Gryseels, K. Struyve *et al*, "*PANEL - Protection Across Network Layers*," Proceedings of the European Conference on Networks and Optical Communications (NOC '97), Core and ATM Networks, D. W. Faulkner and A.L. Harmer, IOS Press, 1997.
- [15] M. Gryseels and P. Demeester, "*Survivability design in multi-layer transport networks*," Proceedings of the 6th International Conference on Telecommunication Systems: Modeling and Analysis, Nashville, March 1998.
- [16] M. Gryseels, S. Ohta, R. Clemente and P. Demeester, "*A Cost Evaluation of Service Protection Strategies in ATM on SDH Transport Networks*," Proceed-

- ings of DRCN 98: 1st International Workshop on the Design of Reliable Communication Networks, Brugge, May 1998.
- [17] M. de Prycker. *“Asynchronous Transfer Mode: Solution for B-ISDN,”*. Ellis Horwood, 1991.
- [18] A. Nagarajan, 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.
- [19] *“SONET Telecommunications Standard Primer,”*
http://www.tek.com/Measurement/App_Notes/SONET/
- [20] *“Dense Wavelength Division Multiplexing,”*
<http://www.techguide.com/comm/sec.html/dwave.html>
- [21] D. E. Comer, *“Internetworking With Tcp/Ip : Principles, Protocols, and Architecture”* Vol. 1, 3rd Edition, Prentice Hall Press, April 1995.
- [22] J. Postel, *“Internet Control Message Protocol,”* Network Working Group, RFC 792, ISI September 1981.
- [23] V. Strazisar, *“Gateway Routing: An Implementation Specification”,* IEN 30, Bolt Beranek and Newman, April 1979.
- [24] *“Types and Characteristics of SDH Network Protection Architectures,”* ITU-T Recommendation G.841, July 1995.
- [25] *“Interworking of SDH Network Protection Architectures,”* ITU-T Recommendation G.842, April 1997.
- [26] J. B. Evans, V. S. Frost, G. J. Minden, *“Service Independent Access Points (SIAP) to Optical Wide Area Networks,”* Gigabit Networking Workshop GBN’98, San Fransisco, March 1998.

- [27] Y. Tada, Y. Kobayashi, Y. Yamabayashi, S. Matsuoka and K. Hagimoto, "OA & M Framework for Multiwavelength Photonic Transport Networks," IEEE Journal on Selected Areas in Communications, Vol. 14, No. 5, June 1996.
- [28] M. Bischoff, M. N. Huber, O. Jahreis, "Operation and Maintenance for an All-Optical Transport Network," IEEE Communications Magazine, October 1996.
- [29] D. Medhi, 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.
- [30] R. Ramaswami, K. N. Sivarajan, "Design of Logical Topologies for Wavelength-Routed Optical Networks," IEEE Journal on Selected Areas in Communications, Vol. 14, No. 5, June 1996.
- [31] N. Wauters and P. Demeester, "Multiwavelength Cross-Connected Networks," IEEE Journal on Selected Areas in Communications, Vol. 14, No. 5, June 1996.
- [32] N. Nagatsu, S. Okamoto and K. Sato, "Large Scale Photonic Transport Network Design Based on Optical Paths," Proc. GLOBECOM '96, London, U.K., November 18-22, 1996.
- [33] K. Murakami, H.S. Kim, "Comparative Study on Restoration Schemes of Survivable ATM Networks," IEEE INFOCOM 1997, Kobe, Japan, April 9 1997.