DIFFERENTIATED QUALITY-OF-RECOVERY AND QUALITY-OF-PROTECTION IN SURVIVABLE WDM MESH NETWORKS

by

Samir Sebbah

A thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of Doctor of Philosophy

Concordia University

Montréal, Québec, Canada

July 2010

Your file Votre référence
ISBN: 978-0-494-71160-6
Our file Notre référence
ISBN: 978-0-494-71160-6

Abstract

Differentiated Quality-of-Recovery and Quality-of-Protection in Survivable WDM Mesh Networks

Samir Sebbah, Ph.D.

Concordia University, 2010

In the modern telecommunication business, there is a need to provide different Quality-of-Recovery (QoR) and Quality-of-Protection (QoP) classes in order to accommodate as many customers as possible, and to optimize the protection capacity cost. Prevalent protection methods to provide specific QoS related to protection are based on pre-defined shape protection structures (topologies), e.g., p-cycles and p-trees. Although some of these protection patterns are known to provide a good trade-off among the different protection parameters, their shapes can limit their deployment in some specific network conditions, e.g., a constrained link spare capacity budget and traffic distribution.

In this thesis, we propose to re-think the design process of protection schemes in survivable WDM networks by adopting a new design approach where the shapes of the protection structures are decided based on the targeted QoR and QoP guarantees, and not the reverse. We focus on the degree of pre-configuration of the protection topologies, and use fully and partially pre-cross connected p-structures, and dynamically cross connected p-structures. In QoR differentiation, we develop different approaches for pre-configuring the protection capacity in order to strike different balances between the protection cost and the availability requirements in the network; while in the QoP differentiation, we focus on the shaping of the protection structures to provide different grades of protection including single and dual-link failure protection. The new research directions proposed and developed in this thesis are intended to help network operators to effectively support

different Quality-of-Recovery and Quality-of-Protection classes. All new ideas have been translated into mathematical models for which we propose practical and efficient design methods in order to optimize the inherent cost to the different designs of protection schemes. Furthermore, we establish a quantitative relation between the degree of pre-configuration of the protection structures and their costs in terms of protection capacity.

Our most significant contributions are the design and development of Pre-Configured Protection Structure (p-structure) and Pre-Configured Protection Extended-Tree (p-etree) based schemes. Thanks to the column generation modeling and solution approaches, we propose a new design approach of protection schemes where we deploy just enough protection to provide different quality of recovery and protection classes.

Acknowledgments

I would like to express my deepest gratitude to my supervisor Dr. Brigitte Jaumard. Her guidance and encouragement made my thesis work a pleasant and extremely educational experience. Her technical and editorial advice and infinite patience were essential for the completion of this dissertation. I feel privileged to have had the opportunity to work with her.

I am also grateful to the members of my thesis supervisory committee Dr. Dongyu Qiu, Dr. Mingyuan Chen, Dr. Anjali Agarwal, and my external examiner, Dr. Dominic Schupke.

Last, but not least, I thank my wife, Ghania, for her understanding and patience during the past few years. This dissertation would not be possible without her support and encouragement. My deepest thanks go to my parents for their self-giving love and support throughout my life.

Contents

List of Figures

List of Tables

List of Acronyms

3R	Re-amplification, Re-shaping, Re-timing
ADM	Add-Drop Multiplexer
APS	Automatic Protection Switching
ASON	Automatic Switched Optical Network
ATM	Asynchronous Transfer Mode
B&B	Branch and Bound
BLSR	Bidirectional Line-Switched Ring
CG	Column Generation
CR-LDP	Constraint-based LAbel Distribution Protocol
dB	Decibel
DCS	Digital Cross-Connect System
DFB	Distributed FeedBack
DFS	Depth First Search
DSL	Digital subscriber line
DWDM	Dense Wavelength Division Multiplexing
DXC	Digital Cross Connect
ESCON	Enterprise Systems Connection
FDL	Fiber Delay Line
FEC	Forward error correction
Gb/s	Gigabit per Second

GigE	Gigabit Ethernet
GMPLS	Generalized Multi-protocol Label Switching
ILP	Integer Linear Programming
IP	Internet Protocol
ISP	Internet service provider
ITU	International Telecommunication Union
LAN	Local area network
LDP	Label Distribution Protocol
LMP	Link Management Protocol
LP	Linear Programming
LSA	Link State Advertisement
LSP	Label Switching Path
LSR	LAbel Switching Router
MAN	Metropolitan Access Network
Mb/s	Megabit per Second
MEMS	Micro-Electro-Mechanical Systems
MILP	Mixed Integer Linear Programming
MPLS	Multi-protocol Label Switching
NE	Network Element
NNE	Network-Network Interface
OADM	Optical Add Drop Multiplexer
OBS	Optical Burst Switching
OEO	Optical to Electrical to Optical
OLT	Optical Line Terminal
OPEX	OPerational EXpenditure
OSPF	Open Shortest Path First
OSPF-TE	Open Shortest Path First with Traffic Engineering

OTN	Optical Transport Network
OTU	Optical channel Transport Unit (OTU)
OXC	Optical Cross Connect
PSTN	Public switched telephone network
PWCE	Protected Working Capacity envelope
QoP	Quality-of-Protection
QoR	Quality-of-Recovery
QoS	Quality-of-Service
RMP	Restricted Master Problem
SBLP	Shared Backup Link Protection
SBPP	Shared Backup Path Protection
SBSP	Shared Backup Segment Protection
SDH	Synchronous Digital Hierarchy
SLA	Service-Level Agreement
SONET	Synchronous Optical NETwork
SRG	Shared Risk Group
SRLG	Shared Risk Link Group
STS	Synchronous Transport Signal
TDM	Time Division Multiplexing
TS	Time Slot
UNI	User-Network Interface
UPSR	Unidirectional Path-Switched Ring (UPSR)
VC	Virtual Circuit
VP	Virtual Path
VPN	Virtual Private Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing

CHAPTER 1

Introduction

1.1 Motivation and Background

The explosive growth of the Internet and the introduction of several new services and applications have created an increasing demand for communications in different domains. Besides the classical IP-based applications, such as web browsing, e-mails, Voice over IP (VoIP), IPTV, Internet games, Video on Demand (VoD), Peer-to-Peer (P2P) services, other services and applications with different stringent Quality-of-Service (QoS) requirements are becoming ubiquitous. Although several broadband technologies have been introduced during the last decades, fiber optics is still the primary technology for broadband connectivity, particularly for communications over long distances. Recent advances in optical signal processing and Wavelength Division Multiplexing (WDM) technology have created many opportunities for multiplexing of several Gigabyte-channels on a single fiber link. The growth of the transport capacity of fibers has been accompanied with the development of optical switching technologies which have enabled flexible and reconfigurable optical cross connects to simultaneously switch hundreds of wavelength channels. This, in turn, has stimulated many network operators to extensive optical WDM technology deployment during the last decades [RI98, LE98]. However, the huge bandwidth capacity brought by optical fibers and switching technologies in WDM networks have raised their vulnerability level to equipment failures. In WDM networks, a single network outage resulting from a link or node failure, even for a short period of time, can lead to a traffic loss of several terabits [Gro04a, VPD04].

Providing resilience against network failures is an important feature in many high-speed networks in order to meet the service availability requirements. As part of Service-Level Agreement (SLA) between network operators and their cooperative customers, operators commit to providing services with different availability guarantees, e.g., 99.999% for the duration of the service, and usually compensation if these are not met. Protection, which involves resource redundancy, e.g., fibers and switching nodes, has been the most widely used resiliency mechanisms in optical networks. In the design of protection schemes, there are many decision parameters that need to be considered before selecting a protection strategy to respond to a specific protection need. Although the main targeted parameter in the design of protection schemes is usually the recovery delay, other parameters such as the deployment cost, scalability, manageability, and flexibility are also targeted in some protection schemes. Indeed, the design objective of a protection scheme in WDM networks is usually a multi-objective function, whose solution constitutes a trade-off among the different involved sub-objectives and parameters.

Protection schemes in survivable optical networks, particularly in WDM networks, have evolved from dedicated to extensively shared protection schemes. The evolution has been motivated by the increasing cost of protection resources needed to provide high reliability and availability to the growing number of applications and services. However, reducing the protection capacity cost comes at the expense of several protection functionalities, among which are recovery delay and management complexity. Thus, many design strategies of protection schemes in the literature have focused on the trade-offs among the involved protection parameters [WAPD01. WSM02, RJ08, Sim07, HS07].

Either shared path. segment or link oriented, various pre-configured protection structures, e.g., linear paths [Muk92a, Muk92b], p-trees [MFB99, XCTT02], p-cycles [GS98], have been proposed in the literature to provide protection in survivable WDM networks. Each of these basic protection structures is associated with a cost in terms of protection capacity, and a recovery delay which depends on its pre-configuration. The *pre-cross connectivity* ahead of failures is a characteristic of some protection structures that enables them to provide protection with a limited reconfiguration in case of a failure. Pre-defined shape protection structures that can be totally pre-cross connected ahead of failures include p-cycles and pre-cross connected trails (p-trails or PXTs) [CCF04a]. In totally pre-cross connected structures, there is a unique way to map each input port to each output port at switching nodes. Thus, pre-mapping is performed ahead of any failure, and dynamic re-mapping is only performed at the end-nodes of failing links. However, as the protection capacity is only allocated following some pre-defined shape topologies, this approach can result in an extra cost due to the limitation of the allocation plan of the protection capacity. On the other hand, dynamically cross connected protection schemes, which involve dynamic cross-connection of protection capacity at switching nodes in case of a failure, can enable more flexible capacity allocation planes. However, this approach has its cost in terms of recovery delay and management overhead. In partially pre-cross connected protection schemes, the number of cross connects that need dynamic reconfiguration at switching nodes and along backup paths is optimized. This approach can achieve a good balance between capacity redundancy and recovery delay.

Those differently pre-configured protection schemes offer different availability guarantees, and require different network resource redundancies. Meanwhile, there is a trend in the design of survivable optical networks toward solutions that will support a variety of applications and services with different availability requirements and costs. Indeed, not all the supported services need the same level of availability, and not all the customers can afford to pay the price of a high service availability. Tough, differentiation of quality of recovery can be a solution for both network operators and customers in order to minimize the protection capacity cost and receive affordable services, respectively. On the operator side, optimization of the protection budget to provide a larger portfolio of services at different rates is an important issue in order to provide competitive services.

Another concern in the design of protection schemes, not much considered, is the ability to provide multiple guarantees of protection, also called Quality-of-Protection (QoP). Mostly designed protection schemes are optimized to protect against single-link failures [TMP05, GC05, TN94, MCL+03, HLS07]. However, since the link-failures are not really independent and do not come one at a time, providing protection against dual-link failures is going to be the next protection level to improve the network availability after a guaranteed 100% single-link failure protection.

Many factors can motivate the need for providing resiliency against dual-link failures in modern communication networks. Single-link failure recovery schemes guarantee 100% protection in case of a link failure within a short recovery time (few milliseconds to few seconds depending on the protection scheme). However, before the physical repair of the failure, it may happen that a second failure occurs, thus, leading to a dual-link failure. Another motivation for investigating dual-link failures is related to the Shared Risk Link Group (SRLG) concept, i.e., a set of optical fiber links that share the same risk of failure. We can also think of network applications and services that are mission-critical, and hence, require 100% availability (say, e.g., tele-surgery) which is not necessarily guaranteed by a 100% single-link failure protection scheme. However, to provide resiliency against all single-link and dual-link failures, it takes an amount of protection capacity proportional to the targeted QoP level (see Chapter 9). In such a case, differentiation of QoP can be the solution for saving protection capacity and providing different guarantees of protection as they are needed. Such as in the differentiated QoR approach, in differentiated QoP, not all users can afford to pay the same price of a high QoP given the associated cost, and network operators should be able to provide different classes of protection to support different users and services with different requirements.

1.2 Research Agenda

Although the recent trends toward the integration of voice and data services have opened up many interesting areas for research, not much work has been done on QoR and QoP differentiation in survivable WDM networks. The associated design problem of protection schemes taking into account different recovery and protection requirements is a multi-dimensional problem that requires efficient optimization and planning tools. Some research efforts have been made in recovery differentiation [GS02, SM04, AKM03, BKLS01, DSST99] where authors have combined some QoS parameters related to recovery and protection. But, only few efficient design methods have been proposed to optimize those designs, accurately evaluate and compare their cost with different network scenarios. and elaborate design strategies that consider the available spare capacity budgets and switching technologies. Furthermore, not much research has considered combination of different protection schemes and logical topologies in order to provide QoR and QoP differentiation in survivable WDM networks. This thesis seeks to help redress this balance by proposing efficient and scalable design methods of protection schemes in order to support QoR and QoP differentiation in survivable WDM networks.

1.2.1 Research Approach

Our design approaches of survivable WDM optical networks supporting QoR and QoP differentiations are based on the shape and connectivity of their protection topologies and oriented to optimize the availability of the supporting networks. Existing protection schemes providing some QoR and QoP guarantees are based on pre-defined shape protection structures, which by their shapes (logical topology) support different protection parameters. For example, p-cycles for recovery delay, and p-trees for local recovery. In this thesis, we propose to re-think the design process of protection schemes in survivable WDM networks by adopting a new approach where we decide the shape of the protection structures based on the QoR and QoP guarantees, not the reverse. In this approach, protection structures (p-structures) of different forms are considered as potential candidates to provide protection, provided that they can effectively meet the different QoR and QoP requirements. We will adopt this design approach in almost the entire thesis.

Our QoR differentiation is based on service availability differentiation. To optimize the network availability, while minimizing the cost of the protection budget, our approach is to develop protection mechanisms based on fully pre-cross connected p-structures, partially pre-cross connected p-structures, and dynamically cross connected p-structures. Those protection approaches achieve different trade-offs among recovery delay, management and signaling overhead, and cost.

Regarding QoP differentiation, provided through single-link and dual-link failure recovery, our approach is based on optimization methods that adapt the shapes of the protection topologies to survive the different failure models associated with the different QoP grades. In our approach, dual-link failures are not improbable and can happen with a given probability. Protection topologies adapted to survive the failure model are elaborated to provide routing diversity in case of any failure. Their shapes are decided based on the failure model.

1.2.2 Research Objectives

Our objectives of this research thesis are to:

- Propose new design approaches of protection schemes, which are cost effective, can provide protection within different network conditions and constraints, and can effectively provide different QoR and QoP guarantees. Though, the spare capacity budget and switching capabilities of nodes will be considered as design constraints. For QoR and QoP differentiations, we propose a multi-availability framework for the design of protection schemes based on fully pre-cross connected, partially pre-cross connected, and dynamically cross connected protection structures, which guarantee different network availability levels and require different protection costs.

- Propose a new design approach of protection schemes in order to provide different QoR and QoP guarantees by using different p-structures. This approach puts the focus on the targeted parameters, and then select the most flexible and effective protection structures, independently of their shapes. Though, for example, fully pre-cross connected schemes are built using all possible p-structures that can be fully pre-cross connected ahead of any failure, independently of their shapes. This in turn, guarantees to select the most flexible structures that, at the same time, will satisfy other design constraints, i.e., link spare capacity budget and traffic distribution.

- In order to be efficient and flexible within different design conditions and constraints, our designs will be based, for both the modeling and the optimization aspects. on a large scale optimization approach named Column Generation (CG). This optimization approach has many advantages, among scalability, efficiency, and flexibility. Though, in this thesis we develop different optimization methods to meet different cost models and satisfy different design constraints.

As the reader will see, all the objectives have been reached and results, which have been obtained, both theoretical and practical, opens new directions for effective designs of protection schemes.

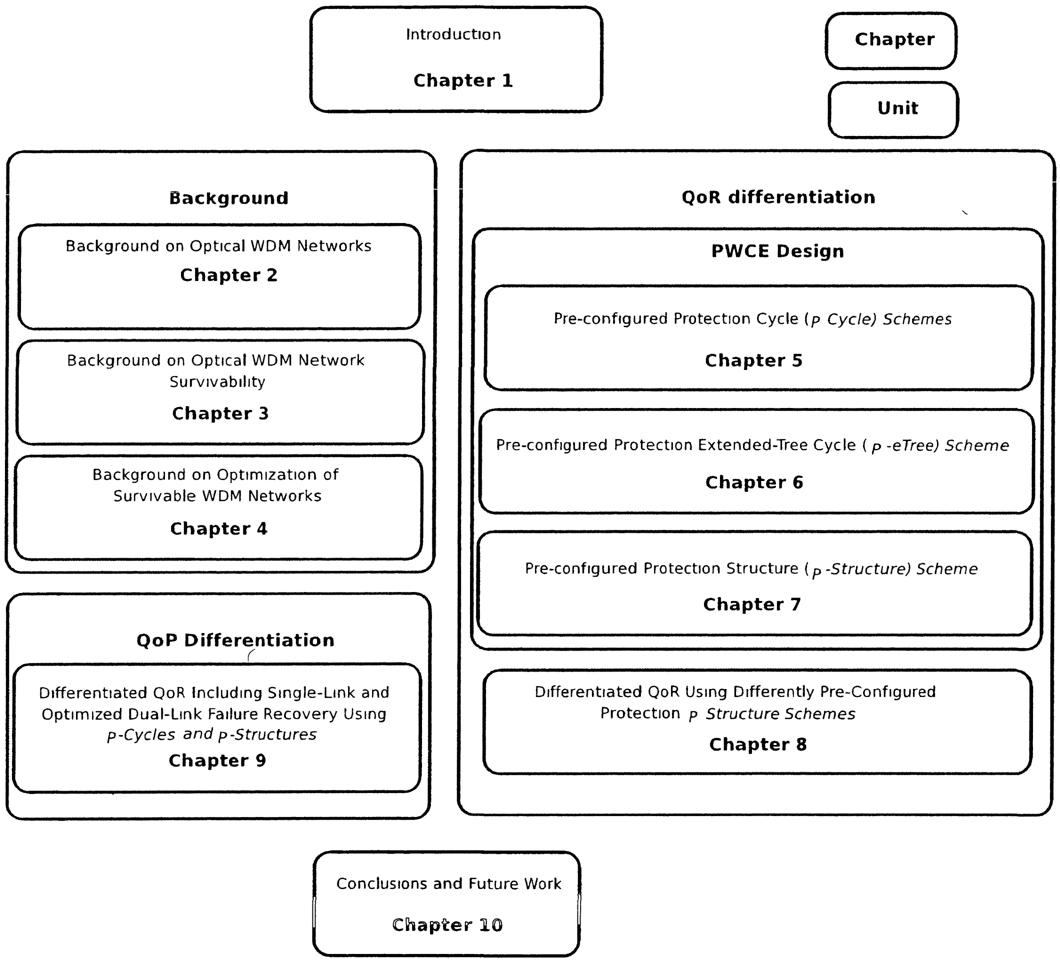


Figure 1.1: Thesis plan

1.3 Thesis Organization

Figure 1.1 illustrates the research plan of the thesis. The entire thesis is divided into three main units: Background, QoR differentiation. and QoP differentiation units.

Chapter 2 provides a brief introduction to transport networks. Two network models illustrating the organization and evolution of transport networks are presented. Three optical architectures of switching nodes - Optical-Electrical-Optical (OEO), transparent, and translucent - are described and compared in terms of scalability and operating cost. The fundamentals of optical control planes including architectures, MPLS/GMPLS techniques are discussed. The focus is placed on GMPLS, and features such as automated provisioning, traffic engineering, link management, routing, and signaling. Finally, the engineering process of WDM systems is briefly reviewed by presenting the involved physical components, discussing the power budgeting problem, and different other design considerations.

Chapter 3 provides background information on survivability in optical networks. First, after a short review of some concepts in the domain, we discuss in details the recovery process in case of a failure. The whole time it takes from the failure appearance to the time of traffic switching is illustrated in a temporal recovery diagram. The spare capacity requirement, signaling overhead, and state overheads, which are among the characteristics of protection schemes are also discussed. In this chapter, we also present the evolution of protection techniques and protection topologies in mesh networks. A brief discussion about multi-layer protection is given with some reviews of existing multi-layer protection approaches in the literatures. Finally, we discuss three different types of protection schemes depending on the pre-configuration of their topologies: The fully pre-cross connected, partially pre-cross connected, and dynamically cross-connected protection schemes. A comparison of some of their protection parameters is presented.

Chapter 4 gives a basic background on optimization in survivable WDM networks. In the first part of this chapter, we review some basic concepts in graph algorithms, and some algorithmic approaches to p-cycles and p-trees searching. In the second part, we focus on Integer Linear Programming (ILP) and Column Generation (CG) optimization techniques. After a review of some ILP solution methods. we present a short introduction to CG modeling and solution approaches.

Chapter 5 proposes efficient and scalable optimization methods based on CG in order to design survivable WDM networks based on simple and non-simple p-cycles in the context of Protected Working Capacity Envelope (PWCE). This chapter is divided into two parts associated with simple p-cycles and non-simple p-cycles, respectively. In the first part. we focus on optimization techniques, and propose an efficient method to maximize the size of the PWCE using different link spare capacity budgets. We compare our approach to a set of ILP-based methods using different enumeration strategies of the candidate p-cycles. In the second part, we propose a new optimization method to extend the solution space of p-cycles and include non-simple p-cycles. Therein, we evaluate the added-value of the non-simple p-cycles with different link spare capacity budgets.

Chapter 6 proposes a new design approach of protection schemes based on hybrid protection structures, we named, pre-configured protection extended-trees (p-etrees). Starting from a p-tree, a p-etree is formed by potentially re-shaping the protection topology of the initial p-tree. The resulting protection pattern of this re-shaping process can be a p-cycle, a p-tree, a p-trail, or any hybrid structure of these protection structures. The motivation behind this construction is to allow those complementary structures to supply their mutual needs and offset their mutual disadvantages. Indeed, the capacity efficiency of p-cycles and their recovery delay can offset the capacity inefficiency and recovery delay of p-trees, and the scalability and flexibility of p-trees can offset that of p-cycles.

Chapter 7 extends further the solution space of the potential protection structures to include all possible patterns. In this chapter, we propose design methods of protection schemes based on p-structures in the context of PWCE. In contrast to the previous protection schemes, in this chapter we do not concern ourselves with the pre-cross connectivity of the protection structures. We focus on the sharing of the protection capacity, and propose two design strategies to maximize the size of PWCEs on a hop-by-hop basis and on an end-to-end basis. In the end-to-end basis, we propose an optimization method based on CG in order to maximize the protected flow circulation among switching nodes.

Chapter 8 proposes a design framework of protection schemes in order to provide different Quality-of-Recovery (QoR) classes in survivable WDM networks. Three recovery classes are associated with three protection approaches using differently pre-configured protection structures. In this chapter. we generalize the p-structure approach. and design protection structures that can be fully pre-cross connected ahead of failures. partially pre-cross connected ahead of failures, and dynamically cross connected in case of a failure.

Chapter 9 proposes a design framework of protection schemes in order to provide different Quality-of-Protection (QoP) classes in survivable WDM networks. Different classes of protection are associated with different protection levels against single-link failures and optimized dual-link failures. In this chapter, we consider both the *p*-cycle and the *p*-structure based schemes. We propose CG modeling approaches that re-shape the *p*-cycle patterns in order to meet different dual-link failure protection scenarios, and study the required spare capacity budget for that. With the *p*-structure scheme, our objective is to identify the most efficient patterns in order to effectively meet the different requirements of protection.

Chapter 10 concludes the thesis and presents some future research directions.

Chapter 2

Background on Optical WDM Networks

2.1 Definition and Evolution of Transport Networks

A transport network can be regarded as a set of equipment and facilities such as switching devices (routers, switches, multiplexers ⋯) and transmission medias (copper cables, optical fibers. Hertzian waves ⋯) carrying client signals. The set of network equipment and facilities, usually referred to as network elements (NEs), provide and support features, functions, and capabilities, which are necessary for transmission of information over the transport network [FCC96].

In order to respond to the increasing needs for high-bandwidth services, fiber-optics technology and WDM switching have been largely deployed in metropolitan and long-haul transport networks [RI98. LE98]. Fiber-optics technology can effectively meet the increasing demand for high bandwidth services, thanks in part to its huge bandwidth, low signal attenuation (around 0.2 dB/km). and low power and space requirements. WDM is the favorite multiplexing technology in multi-wavelength optical networks because it supports a cost effective transmission of a large number of concurrent transmissions of optical channels. Huge bandwidth capacity can result from multiplexing of several wavelengths on a single strand of fiber, e.g.. a fiber that can support up to 160 channels operating at 40 Gb/s would yield an aggregate of 6.4 Tbps.

There has been a growing trend toward integration of different types of networks (i.e., data, voice, and multimedia/video) in the recent telecommunication business. The key driver behind integration is the reduction of the capital equipment costs by avoiding multiple overlay networks and reducing inherent Administration, Operation, Maintenance and Provisioning (OAM&P) costs. However, as transport networks grow in geographical size, connectivity, and capacity, it becomes increasingly impossible to manage them with any degree of reliability or cost effectiveness. Hence, logical decomposition of the whole network into smaller networks in order to simplify its AOM&P has been adopted.

2.1.1 Geographical Hierarchy of Transport Networks

Based on their geographical scope, transport networks can be divided into three categories: access (spanning about 1 to 10 km) metropolitan (covering about 10 to 100 km), and long-haul (extending to 1000s km). These categories are illustrated in the three-level hierarchy in Figure 2.1 (adapted from [Sum05]).

The access network is the portion of the network that connects end-users (customers) to the edge switching elements in the transport network. Residential cable networks, cellular networks, Gigabit Ethernet networks, Corporate LANs, and regional ISPs are some typical access networks. The Metropolitan Network (MAN) is the portion of the transport network that interconnects central offices (COs) within suburban or urban areas. MANs are typically the networks that collect the traffic from the access networks and route it onto the long-haul transport network. Inter-metropolitan connections also exist in order to perform local traffic routing. The long-haul core transport network provides connections between metro networks through regional and international gateways.

2.1.2 Layered Architectural Model

The demand for high bandwidth in transport networks increases from the access networks to the long-haul networks. This hierarchical organization and the ever-increasing demand for high bandwidth have shaped different technological aspects of transport networks. Another useful network

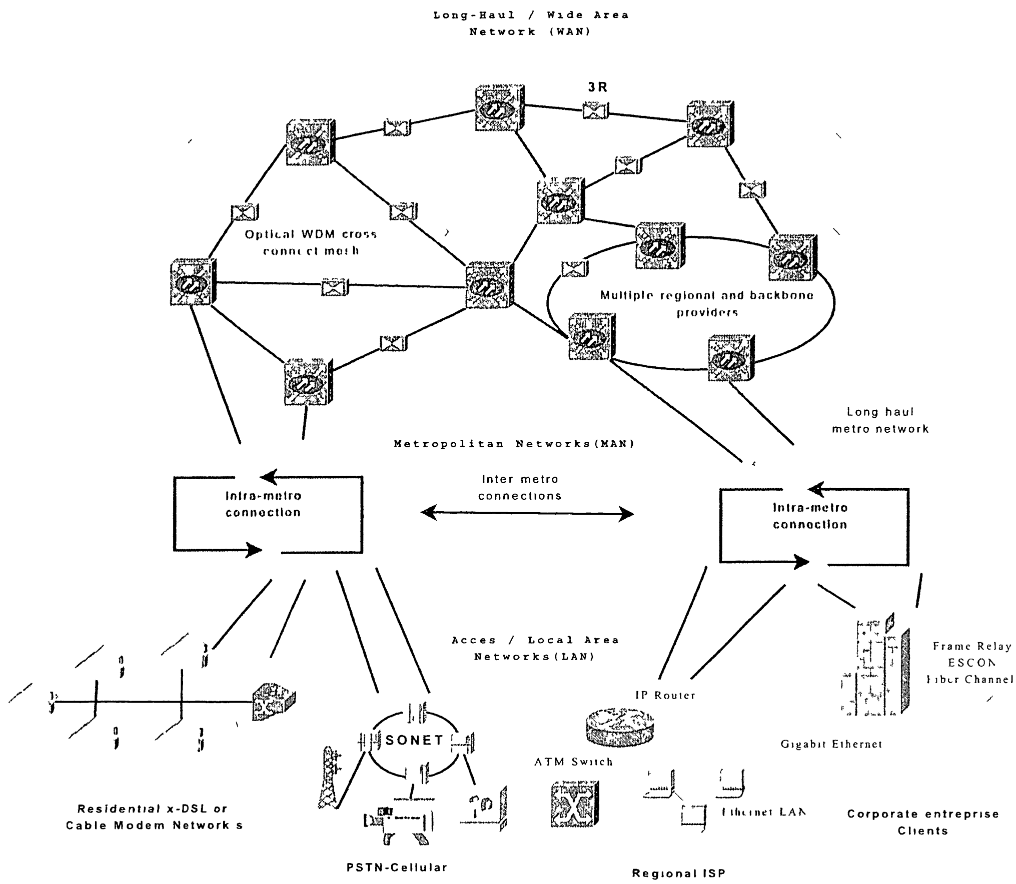


Figure 2.1: Hierarchical Transport Networks

classification is illustrated by the three-layered model in Figure 2.2. At the top of this hierarchical model is the service layer where the different applications and services such as voice, video, and data are offered. The intermediate layer is the service infrastructure layer where routing, multiplexing and switching of upper layer services are performed. This layer includes Internet Protocol (IP) routers, Ethernet switches, and Time Division Multiplexing (TDM) facilities. At the bottom of the hierarchy is the transport layer which constitutes a hierarchy of transport sub-layers on top of a physical layer e.g., WDM-based Optical Transport Network (OTN). In this layer, multiplexing of finer granularity services is performed in order to optimize the transport capacity of the optical layer.

In this hierarchical architecture, each sub-layer is characterized by the granularity at which the bandwidth is managed. With the introduction of several high bandwidth services and the integration of multiple data and multimedia networks onto a single transport infrastructure, the multiplexing and switching facilities have greatly evolved over the time in order to meet the increasing demands of

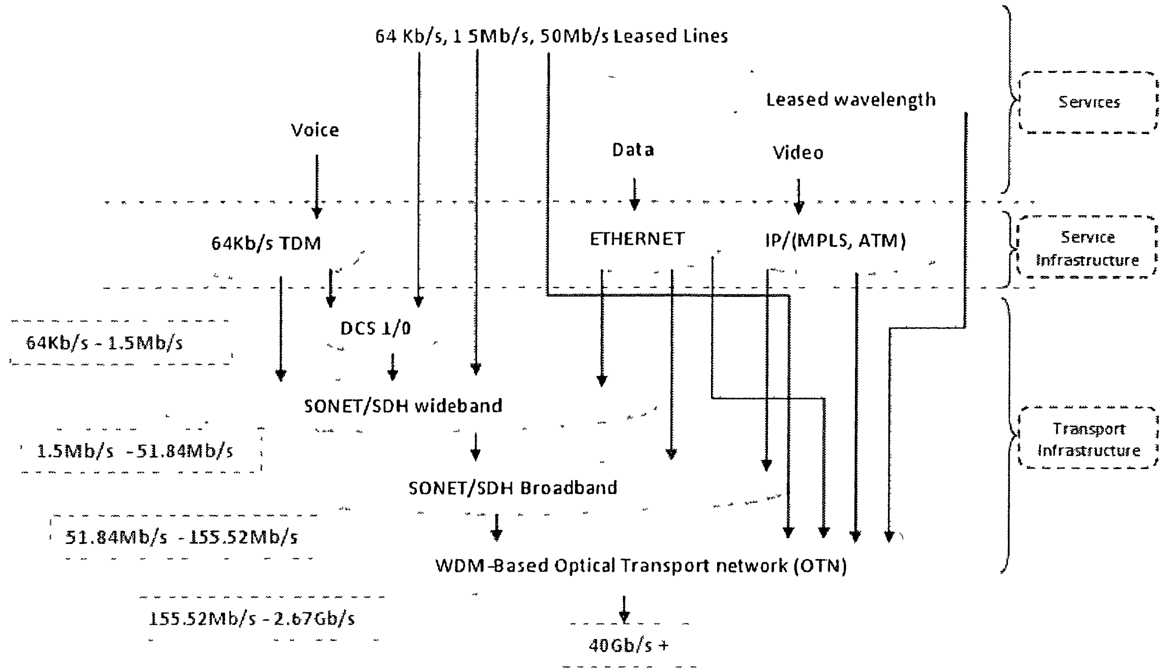


Figure 2.2: Transport Infrastructure Layers

high bandwidth. The 1.5Mb/s sub-layer was introduced in order to ease bandwidth management and meet the needs of elementary services in terms of bandwidth. Similarly, higher bandwidth services were introduced and the fiber optics technology made it possible to carry signals at 51.84Mb/s (SONET STS-1). Multiple SONET STS-1 signals are multiplexed together to form higher rate SONET signals, giving a SONET hierarchy rate. In Figure (2.2) three STS-1 are multiplexed to form an STS-3 of 155.52 Mb/s. The optical instance of a general STS-N signal is called the Optical Carrier level-N, or OC-N. However, the rapid growth of the service and service-infrastructure layers have urged the development of new transport standards. Moreover, IP and ATM switch vendors are already introducing switching solutions at several Gb/s to Tb/s [KCY$^+$03], and the capacity of the new Ethernet standard has reached the threshold of 100Gb/s [D'A09]. Furthermore, some specific users may require to directly access the optical layer as illustrated in Figure (2.2). Such a capability is desirable in some situations to transfer large and steady streams of protocol and format-independent data. The WDM layer complements the transport hierarchy by providing coarse granularity bandwidth (wavelengths) management to the finer granularity sub-layers. A wavelength in the WDM layer is not constrained by a fixed-rate, or multiplexing protocol; it can carry any protocol, such as SONET, IP, and Ethernet, and any bit-rate, such as, 155.5Mbs, 1.25Gb/s and 40Gb/s. Furthermore, the protocol and the bit-rate of the streams carried on a given wavelength can be adapted dynamically without changing much the transport infrastructure.

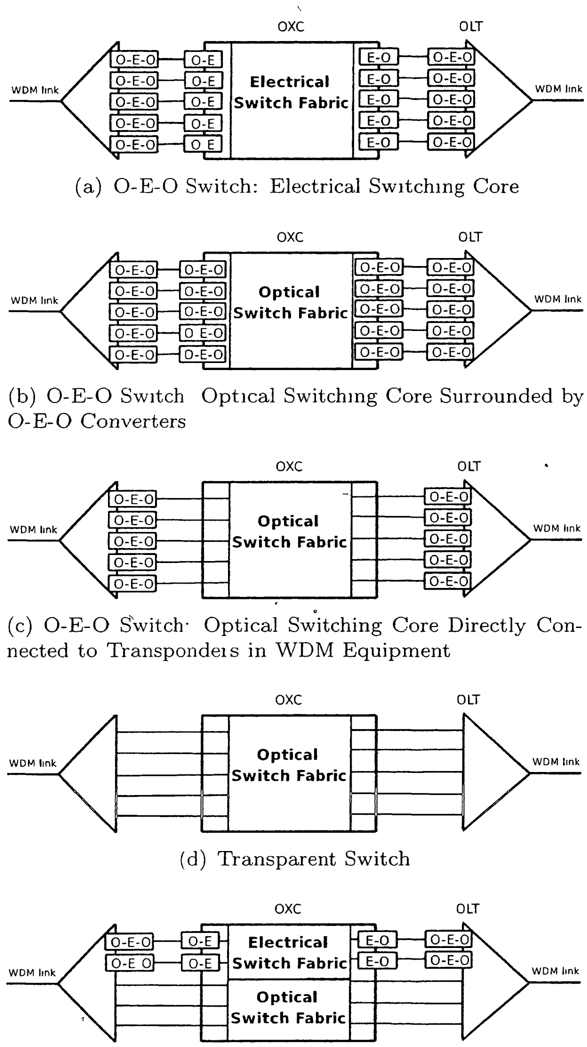
In order to provide more efficient use of the transport capacity in the WDM layer by the upper layers, the ITU has recently developed a new hierarchical transport paradigm, called the Optical Transport Network (OTN) [Uni03, Uni01]. The hierarchy and formats are defined in the ITU standard $G.709$ where the basic frame is called an Optical channel Transport Unit (OTU). The bit rate of the OTU hierarchy is slightly higher than the ones of the classical SONET/SDH, the basic OTU1 offers a rate of 2.67 Gb/s, and the OTU2 and OTU3 offer 10.71 and 43.02 Gb/s, respectively. Compared to SONET/SDH, OTN provides efficient and flexible switching and multiplexing of high-bandwidth services and stronger forward error correction (FEC) capabilities. It is envisioned as a step forwards network convergence, where operators can support a large portfolio of services with a single technology rather than multiple overlapping networks. Furthermore, OTN can greatly improve the network survivability by reducing the number of opto-electrical devices, which constitute a major source of equipment failures.

2.2 Optical Switches

An optical switch is a device that enables signals in optical fibers to be selectively shifted from one circuit to another. It is composed of an Optical Line Terminal (OLT), which is formed of transponders, wavelength multiplexers, and optionally, optical amplifiers, and a switching matrix, also known as an Optical Cross Connect (OXC) or *switch fabric*. The main function of an optical switch is to map input/output channels in order to enable optical circuits (see Figure 2.3) through the switch. The established circuit at all the switch nodes from the source to the destination of a communication is known as a lightpath [CFZ96].

Figure 2.3 shows different types of optical switches, i.e.. different OXC and configurations for interconnecting OXCs with OLTs in a switching node. The switch fabric where the input/output ports are mapped is the heart of the optical switch. There is a broad class of optical switches, and they are usually named after the operating domain of their switch fabric and OLTs. However, contrary to what the name "optical switch" may let suppose, these switches do not necessarily have a switch fabric that operates on optical signals. Rather, the term optical switch refers to the switch where the ports operate on the granularity of a wavelength or waveband (group of wavelengths).

Based on the domain of operation of their interconnected components, optical switches can be divided into three categories: O-E-O switches, transparent switches, and translucent switches.



(a) O-E-O Switch: Electrical Switching Core

(b) O-E-O Switch Optical Switching Core Surrounded by O-E-O Converters

(c) O-E-O Switch· Optical Switching Core Directly Connected to Transponders in WDM Equipment

(d) Transparent Switch

(e) Translucent Switch

Figure 2.3: Optical Switch Architectures

2.2.1 O-E-O Switches

An optical switch based on O-E-O, also known as *opaque* switch, is shown in Figures 2.3-(a)(b)(c). These three architectures are all opaque architectures, i.e., optical signals are converted into the electrical domain as they pass through the switching node. In these three configurations, the OXC can be either electrical or optical, i.e., signals are either switched in the electrical domain or the optical domain. The electrical OXC of Figure 2.3-(a) provides some functionalities that are not available in the optical OXC of Figures 2.3-(b)(c), such as, grooming of low fine granularity wavelengths and Time Division Multiplexing (TDM) of different speed streams.

An optical switch is considered as an O-E-O device if the optical signals passing through undergo optical-electrical conversion, i.e., one of its component is equipped with converters and transponders, either its OLTs, or OXC. There are some advantages inherent to the switching technique in the O-E-O architecture. First, converting the optical signal to the electrical domain and back to the optical domain helps in regenerating the signal. Optical signals experience degradation as they are transmitted along a fiber. By regenerating the signal through electrical conversion, the O-E-O technique enables re-amplification, re-shaping, and re-timing (3R) of the optical signal. Second, it improves the performance monitoring of the signal, by allowing efficient error correction and accurate failure location. Third, O-E-O provides flexible wavelength allocation by allowing wavelength conversion at the switching nodes. Wavelength continuity, which is the constraint that imposes to the output wavelength of a signal to match its input wavelength, is a challenging issue in optical switching networks. The problem of provisioning connections with wavelength continuity and limited wavelength conversion constraints is a challenging issue that has attracted many researchers [ZJM00, BM96]. In the O-E-O architecture, optical switches electrically process and switch the received lightpaths, thus wavelength conversion is implicitly enabled. Furthermore, traffic grooming and traffic engineering are among other functionalities that are enabled in the O-E-O architecture. However, because every wavelength is terminated at every switching node poses serious problems of scalability, maintenance, and reliability. Indeed, as capacity grows, such an architecture could potentially require hundreds of transponders at each node. Which implies larger spaces at the site housing the equipment, and more power to operate the electrical equipment and dissipating the heat created by them. In addition, capacity upgrade is a costly operation that usually requires updating of many facilities. For example, an interface that supports a 10Gb/s typically does not also support a 40Gb/s signal. Furthermore, all the equipment required in the O-E-O architecture is potentially prone to failures. This increase the network vulnerability, though, decrease its reliability.

2.2.2 Transparent Switches

The term *transparent switch* (also called photonic or all-optical switch) refers to an optical switch where the switch fabric operates on optical signals and the incoming optical lightpaths do not undergo optical-electrical-optical conversions. Figure 2.3-(d) illustrates an example of a photonic switch that is used to switch optical signals in the optical domain.

In this architecture, the interfaces of the switch fabric are removed as the signals are optically switched. Only a couple of technologies used in the fabrication of photonic switches have appeared in deployed optical networks. The leading technology is based on 3D Micro-ElectroMechanical Systems (MEMS). 3D MEMS uses control mechanisms to dynamically tilt mirrors in multiple directions (3D) Due to their physical properties, i.e., low loss, cross-talk, polarization effect, power consumption $\cdots$ (see Table 2.1), MEMS is currently holding the promise of providing and managing all-optical switches that support a large number of optical lightpaths without converting them to electrical and back to optical again [MK03]. This is especially attractive in transport networks where a high percentage of traffic is expected to pass through different switch nodes to its destination.

The benefits of all-optical includes deployment and operating costs. The deployment and operational costs, also known, as CAPital EXpenditure (CAPEX) and OPerational EXpenditure (OPEX) are the two budgets that all network operators want to minimize through deployment of all-optical architectures. Photonic switches are bit-rate and protocol independent. i.e., they can support different wavelengths and transport protocols These features have improved the flexibility of optical networks by allowing wavelength service allocation without the intervention of a human operator

The main challenge of All-Optical Networks (AON) is the optical signal reach In addition to the

	Free-space		Guided wave	
	MEMS	Liquid crystal	Thermo-optic Bubble	Thermo-optic/ Electro-optic waveguide
Scalability	√	×	×	×
Loss	√	?	×	×
Switching time	√	?	?	√
Cross-talk	√	?	?	?
Polarization effects	√	? √	? √	×
Wavelength Independence	√	√	√	×
Bit rate Independence	√	√	√	√
Power Consumption	√	√	×	×
√:good, ?:unsure, ×:bad				

Table 2.1: Optical Switches: Photonic Fabrics

different physical impairments. all-optical switching fabrics induce power losses ranging from 5 to 15 decibels (dB), depending on the technology used to implement the switching function, the size of the fabric, and the architecture of the switch [RSS09]. At this time, engineering of an optical system that can handle all the network impairments and provide end-to-end lightpaths with a guaranteed quality is a very challenging issue.

2.2.3 Translucent Switches

Figure 2.3-(e) illustrates a translucent optical switch where an O-E-O and transparent fabrics are combined together to form a translucent optical switch. These two architectures can be used to mutually offset their disadvantages in terms of scalability and flexibility. By combining both the O-E-O and photonic fabrics in building switching nodes, operators can extend the optical signal reach limitation, and minimize the CAPEX and OPEX related to electronics. The translucent architecture brings another degree of flexibility to modern transport networks by allowing both bandwidth-based services through O-E-O switching fabrics and bandwidth-based services through photonic switching fabrics. Together the two switching architectures will provide scalability. manageability. and higher flexibility in bandwidth allocation.

2.3 Optical Control Planes

In Figure 2.2, we present a hierarchical optical network from the point of view of services and infrastructures. The focus in this figure, is on the optical transport layer and on the transport in the logical layers (e.g., IP, MPLS). In addition to these transport planes, in optical networks, we can distinguish two other planes: *control and management* planes. In an optical transport network, the transport plane deals with the physical transport of traffic, the control plane provides the intelligence required in the provisioning of connections and their maintenance, and the management plane deals with performance monitoring, failure, security, and accounting management [BRS03].

The current development in optical network control/management has been motivated by the need for unified procedures to coordinate the multivendors equipment. Therefore, an optical switch is very often equipped with a controller in order to coordinate its actions with other switching nodes. To achieve an interoperability among the multivendor equipment, the following facilities are required:

- A routing protocol for topology and resource discovery, route computation, and state information maintenance.
- A signaling protocol to set up, maintain. and tear down connections,
- A signaling network that will support the signaling protocol.

There are three interaction-models between the logical layers (e.g., IP) and the optical layer elements that are responsible of providing end-to-end connectivity. These models are the overlay, peer, and hybrid ones (see [RPS+00] for further readings). These interaction models are different from each other in the way that the routing and state information are shared between the two layers. However, another interaction model is the one between the control entities in the control plane. A standardized method to routing and signaling is an important for automated service provisioning, interoperability, and scalability. In IP networks, a standardized control plane. based on MPLS, has already been widely used, and a Generalized version of MPLS for optical networks that include advanced mechanisms for resource advertisement, signaling. and routing is also available.

2.3.1 Control Plane Architecture

Management and control of large networks are not easy tasks, and decomposition of the entire domain into smaller administrative domains is usually performed in order to simplify their administration. Figure 2.4 shows an optical network divided into two control domains, each with its control layer and interfaces (adapted from [SRB03]). The User-Network Interface (UNI) is the control interface between a node in the optical network and a node in the client network. Network-Network Interface (NNI) is the interface between two control nodes belonging either to the same (Interior) control domain (I-NNI) or different (Exterior) control domains (E-NNI). The control plane connectivity is not necessarily the same as the optical transport plane, i.e., switching nodes that are physical adjacent in an optical network are not necessarily adjacent in the control network. Furthermore, not all optical transport nodes are equipped with a control node, and not all control nodes can make decisions. For example, in a centralized control architecture, a single control node makes decisions and dictates them to other switching nodes.

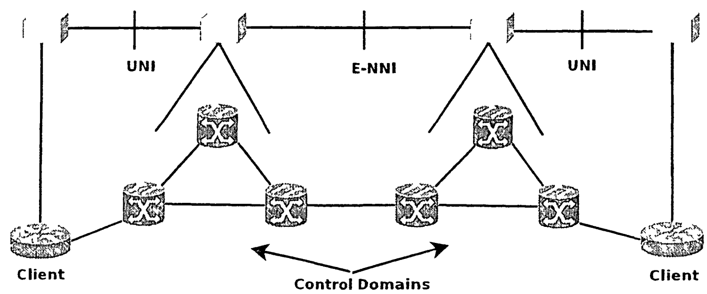


Figure 2.4: Control Plane Architecture

In the control plane, when a request for a connection is received at a given network node, the local routing agent will check its routing databases to find out about the availability of resources before initiating the connection. Keeping track of the availability of resources (either local or global) is performed through exchange of routing information (e.g., availability) between the control agents. Once the availability of resources is verified, a standard signaling protocol is used to establish the computed end-to-end path in the network. The MPLS and GMPLS are two standards that have been widely used for network control.

2.3.2 Multi Protocol Label Switching

MPLS was originally developed for connectionless IP in order to support connection-oriented communications in packet-switched networks. However, as its name implies, it can operate in conjunction with different other protocols. It is used to provide automated provisioning, and to address the issues of scalability, QoS, and traffic engineering in IP networks. MPLS simplifies provisioning by introducing new scalable switching mechanisms, which enabled multiple features such as Virtual Private Network (VPN) and multicasting.

As opposed to IP networks where routing is performed through a heavy header processing, MPLS routing is performed through label swapping (replacing) at every router. To initiate an MPLS session, traffic entering an MPLS network is first encapsulated in special labels at the first MPLS node (switching nodes in MPLS are also known Label Switching Router (LSR)) in the network. A sequence of labels, appended and swapped to and from a packet at each LSR from its source to destination define a Label Switched Path (LSP). The assignment of packets to LSPs is based on the concept of Forwarding Equivalence Class (FEC), which is a set of packets that share, for example, the same destination or QoS requirements. The establishment of LSPs is performed by exchanging information among the LSRs by using a label distribution protocol. An example of label distribution protocol used in MPLS is the Label Distribution Protocol (LDP), which assigns labels to LSPs based on the destination address of the flow. An extended version supporting QoS and Class-of-Service (CoS) features is the Constraint-based Routing Label Distribution Protocol (CR-LDP). The Resource Reservation Protocol with Traffic Engineering extension (RSVP-TE), which is an extension of the RSVP protocol in IP networks, has been adopted in MPLS in order to guarantee QoS requirements and to meet the traffic engineering objectives.

2.3.3 Generalized Multi Protocol Label Switching

GMPLS has extended the control plane in MPLS to support wavelength routed optical networks as well as many other types of networks [FB06]. In addition to some specific packet-switching protocols (e.g.. packets in IP, cells in ATM) supported in MPLS. GMPLS supports labels adapted to arbitrary technologies in the physical layer. For example, labels can be associated with time slots in TDM and SONET/SDH, with wavelengths and wavebands in wavelength/waveband switching networks, and with ports in fiber routing (space) networks. Such an extension makes it possible to manage network elements, provision connections with automated protection and restoration across network boundaries, and support traffic engineering. In the migration process from MPLS to GMPLS, the control plane has been dissociated from the data plane in GMPLS, and the signaling, routing, and label distribution protocols in MPLS have been extended to support dynamic routing of protection/restoration capabilities in mesh networks, and link management has been added in GMPLS as a new management feature. GMPLS has three main components.

Link Management in GMPLS

GMPLS supports link management, a new function, which includes neighbor discovery and management of signaling mechanisms for provisioning and fault recovery. Automated neighbor discovery is important for acquiring the topology and other state information needed for signaling and provisioning of connections. In addition, any change in the network topology or resource availability can be quickly advertised to all routing nodes in the network. This, in turn, guarantees that connections will be efficiently provisioned with up-to-date state information. Link Management Protocol (LMP) is the mean used for implementing the neighbor discovery functions in GMPLS. The control network can be set up in-band (e.g.. using the SONET overhead bytes) or out-of-band in transparent networks through a dedicated control wavelength. In order to manage the number of advertised control messages in the network, GMPLS uses a summarization technique known as "link bundling". In link bundling. all links having the same routing properties are grouped in a single logical group called a "bundle" or "traffic engineering" (TE) link.

Routing in GMPLS

The routing algorithms initially used in IP networks are currently used in GMPLS. However, some new extensions and considerations have been added in optical networks. Among the most important considerations, there is failure-protection and link properties. The routing process in GMPLS has been extended to include the concept of Shared Risk Link Group (SRLG) in the network; and several link properties are included, e.g., transmission impairments, wavelength conversion availability, switch cross-talk. Such extensions have made routing more complex in GMPLS than in IP and MPLS networks, i.e., involves more routing information, and complex routing strategies. These aspects of routing in GMPLS are still under exploration.

Open Shortest Path First (OSPF) has many attractive features, which make it the most used routing protocol as an Interior Gateway Protocol (IGP). Some problems have been addressed in GMPLS to extend it to include routing in optical networks using an enhanced version of OSPF with Traffic Engineering (OSPF-TE). Though, link bundling has been proposed to minimize the number and size of exchanged Link State Advertisement (LSA), specific optical network routing information (number of wavelengths, channels) and protection (SRLG, link protection type) are added, and routing information related to transparent optical networks, e.g., wavelength continuity, signal quality are also advertised.

Signaling in GMPLS

GMPLS signaling involves establishment, maintenance, and releasing of service connections [Ber03a] in optical networks. Current GMPLS implementations are typically based on RSVP-TE. In GMPLS, the *Path* and *Resv* messages used in MPLS are still used in provisioning connections. Figure 2.5 shows a typical connection provisioning session in MPLS (used also in GMPLS). A source node of a connection issues a path message to the destination to indicate the traffic requirements of the communication session. The intermediate routers that process the message create a path state (including information about the sender. traffic characteristics, QoS, identity of the previous hop) for the session, and forward the message to the next hop. At the destination node, a *Resv* message is sent back to the previous node along the path message in order to reserve the required resources. Each intermediate node on the reverse path also reserves the resources and forward the Resv message to its reverse node. After the reservation is completed, the data starts to flow on the established path with the required QoS parameters.

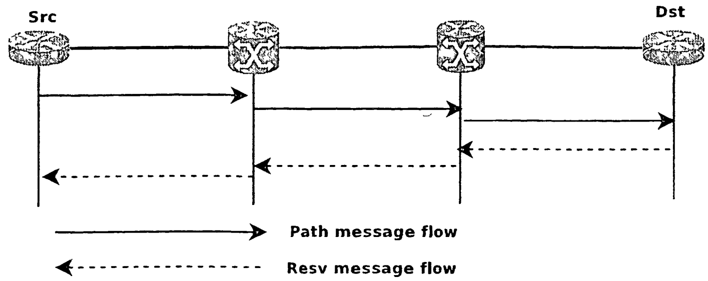


Figure 2.5: Path and Resv Message flows in RSVP

Optical networks can accommodate a variety of multiplexing and switching technologies, e.g., SONET/SDH, wavelength and waveband. To support those different technologies, new label formats and requests are added in RSVP-TE (see [ASBB+01] for further reading). GMPLS signaling in protection capacity networks is reviewed in Section 3.2.1 with an illustrative example of the signaling process.

2.4 Engineering of Optical Fiber Systems

The problem of engineering a WDM transmission system involves several physical components, different design constraints, and a variety of variables in the objective function. Figure 2.6 shows a diagram of the main components of a unidirectional WDM link. Therein, the transmitter is composed of a set of lasers emitting WDM signals on each wavelength. The different WDM signals are combined by a multiplexer onto a single WDM link (fiber). An optical amplifier is usually used to boost the signal transmission power. Depending on the distance, the multiplexed optical channels may be amplified by an in-line amplifier. Usually, at each power amplification, the amplified signals are passed through a dispersion-compensating module. At the receiver end, the optical signals are usually re-amplified before they are de-multiplexed and passed each to a separate photodetector receiver.

As an input, fiber designers dispose of a set of optical components such as transmitters, fibers, receivers, amplifiers ... each characterized by a set of different parameters and by their costs; and design conditions (single link, multi wavelength system). As an output, the resulting engineering

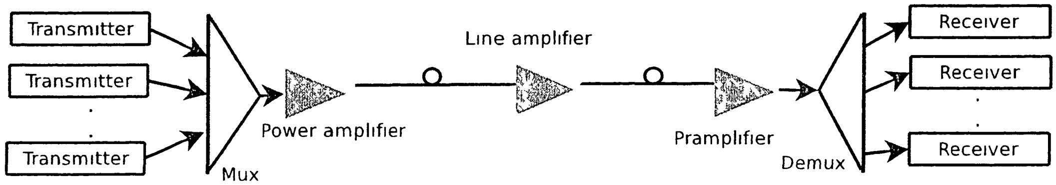


Figure 2.6: Point-to-Point WDM Link

should meet a limited budget (low cost), guarantees a minimum QoS (e.g., bit error rate less than 10^{-12}); and a minimum level of reliability (e.g., should operate without interruption for at least 3 years). However, whatever the complexity of the engineered system, the involved variables are resumed as follows [Hec98].

- Light source output power
- Coupling losses
- Spectral linewidth of the light source
- Type of fiber (single or multimode)
- Fiber attenuation and dispersion
- Fiber core diameter
- Operating wavelength
- Optical amplifiers
- Switching requirements
- Receiver sensitivity
- Number of couplers, connectors, and splices
- Wavelength spacing and number of wavelengths.

2.4.1 Power Budgeting

Designer of optical physical layers must consider the effect of a number of system impairments. A design of an optical communication system requires a careful budgeting of the power for the different impairments in the system. In power budgeting, a designer will deal with the needed power budget in order to cover all optical transmission losses and convey the optical signal to its destination with the required bit error rate. The simplest form of the power budget can be written as follows [Hec98]:

$$Power_{Tx} - Power_{lost} + Power\_Gain_{amplifiers} = Power\_Sensitivity_{Rx} + Power\_Safety\_Margin$$

where the power unit is decibels or any other related unit such as dBm.

$Power_{Tx}$: Transmitter power used in launching the optical signal.

$Power_{lost}$: All losses in the system, e.g., fiber loss, coupling loss. connector loss, $\cdots$.

$Power\_Gain_{amplifiers}$: Power gain of the used amplifiers.

$Power\_Sensitivity_{Rx}$: Power sensitivity of the receiver. Below this level, the signal may not be readable, or meet the minimum bit error rate.

$Power\_Safety\_Margin$: Power margin which is used in compensation for signal fluctuation and repair. It is used to avoid that the power signal fall below the receiver sensitivity.

These characteristics of optical components and their related impairments are covered below.

Optical Transmitters

The key design parameters related to an optical transmitter is its output power. Typical lasers send out about $1mW$ to $10mW$ of power. Typically, some power amplifiers are used to boost the power level of the signals. this typically can be up to 50 mW. Laser sources are physically limited by their peak transmission power. However. this is not the only limiting factor. but other impairments due to nonlinear effects in fibers also set a limit on the peak power of transmitters.

Optical Receivers

The key parameters of an optical receiver are its sensitivity and overload parameter. The sensitivity is the average power required to achieve a certain bit error rate at a given transmission rate. The overload parameter is the maximum input power a receiver can support. A typical sensitivity and overload parameter of an avalanche photodetector (APD) receiver operating at 1.55μm and 1 Gb/s are -24 dBm and -6dBm, respectively [RSS09]. On the receiver side, there are different trade-offs among received power, signal rate, and bit error rate. As data rate increases, the receiver will need more input power to support the specified bit error rate. However, an increase in power is not always the solution to keep the bit error rate low, too much power can overload the receiver and lead to high error rate too.

Optical Amplifiers

Amplifiers are essential components in optical transmission systems to compensate for the different system losses by boosting the signal power. The most widely used is the Erbium-Doped Fiber Amplifier (EDFA) operating in the $C-$band. The advantage of EDFAs is that they are capable of amplifying many channels, e.g., parallel WDM channels. However, an amplifier like other active components is not a perfect device. There are some imperfections optical network designers should consider when using amplifiers. In addition to providing power gain, amplifiers introduce noise too. Furthermore, for high input power, amplifiers tend to saturate and their gain drops. Other limitations include uneven amplification over the entire passe-band. Thus, some specific wavelengths see more gain than others.

Optical Fibers

There are two categories of optical fibers: single-mode and multi-mode fibers. Single-mode fibers are manufactured with a small core size, approximately 8 to 10 μm in diameter. Multi-mode fibers are manufactured with a core size of 50 to 62.5 μm in diameter. This standard is important for interoperability among different industrials. The key optical performance parameters for fibers are attenuation and dispersion.

Attenuation is the reduction of the signal strength over the length of the fiber, and it is measured in decibels per kilometer (dB/km). Optical fiber offers superior interference immunity to signal, e.g., a typical value of 0.35 dB/km at 1300 nm for standard single-mode fiber over other transmission media. This enables signal transmission over longer distances while reducing the signal regeneration and amplification. This, in turn, helps in reducing the engineering cost and improving the signal quality. Attenuation is caused by several factors, but mainly by scattering and absorption. The scattering of light is due to molecular irregularities (compositional fluctuations) in the glass structure. Light absorbed is another attenuation factor caused by residual materials composing the fiber, such as metals or water ions.

Dispersion is the time distortion of an optical signal which typically resulting in pulse broadening. In a digital transmission, dispersion limits the maximum data rate, the maximum distance, or the information-carrying capacity of a fiber link. Chromatic dispersion, which is the most common dispersion, occurs because the refractive index of the fiber is different for all wavelengths. Thus, different wavelengths of the same mode may travel at different speeds, and thereby may cause pulse spreading.

2.4.2 Fiber Optics Impairments and WDM Systems

Fiber dispersion and attenuation are more complex issues when the fiber transmits signals of different wavelengths. Because, their effects vary with the transmitted wavelengths, i.e., although they share the same fiber, they will not necessarily experience the same attenuation and dispersion.

Fiber attenuation varies significantly across the usable waveband from 1280 to 1650 nm. Attenuation is about 0.35db/km in the 1310-nm compared to the minimum near 0.2 bB/km in the EDFA. This difference in wavelength attenuation has an impact on WDM systems operating on the entire light-band range. Light dispersion depends also on the used wavelengths, and engineering of dispersion compensating mechanisms should take into consideration the whole used light-band with their different wavelength dispersions.

Nonlinear effects are proportional to the power density of the signals transmitted in a fiber and to the length of the fiber. Long-haul WDM networks are the most affected networks by these effects, because the power density increases with the number of wavelengths.

2.4.3 Inter-Channel Spacing in WDM Systems

Inter-channel spacing is a WDM design choice that needs a careful engineering. The transmission capacity of a WDM system depends on the number of usable wavelengths, their capacity, and spacing between them. The number of available wavelengths depends on the available amplifiers in the systems, while their spacing greatly on their capacity. We know that the spectral bandwidth of optical channels increases with the data rate it carries. Though, high-speed signals cannot be packed as tight as low-speed signals. However, and in order to take advantage of the optical amplifiers used in the system, optical channels should be within the pass-band of the amplifiers. For example, the C-band EDFA amplifiers are typically from 1530 to 1565 nm.

2.4.4 Photonics Networking

The different aspects of optical system design discussed above apply for point-to-point links as well as photonic networks. However, designing a photonics network is more challenging than a point-to-point link for the following reasons [RSS09]:

- Since photonic lightpaths traverse multiple links and nodes, their optical reach is longer than the reach of a point-to-point link. Thus, end-to-end lightpath engineering involves more constraints than a point-to-point link, such as, losses, and dispersions, which are not reset at each node as in point-to-point link systems.
- The variation of signal power and signal-to-noise ratios among different lightpaths traveling through different numbers of nodes and having different lightpath lengths is a new challenging issue in photonic networks.
- Rapid and dynamic equalization of the amplifier gains will be needed to compensate for fluctuation in optical power as lightpaths are taken down or set up, or in the event of a network

failure. This issue needs to be considered more carefully because it is the key to any dynamic provisioning of working or protection capacity strategy.

2.4.5 Discussions

As seen in this section, in order to set up a single point-to-point link, one needs to carefully engineer a system that involves several components and parameters. In today's optical networks, establishing a single optical link is not a trivial task, and it is largely a manual process. There are so many impairments that need to be set to an appropriate level for a communication before the communication starts.

In the literature, and in order to simplify network design, the tendency is to abstract all those imperfections related to the optical fiber system. The general assumption is that the WDM transmission system can automatically support hundreds of wavelengths, and dial-up end-to-end optical paths by simply concatenating optical links (all optical) on the fly to form working and protection paths However, with the current state-of-the-art of optical fiber and switching, it is not realistic to assume that on-the-fly concatenation of optical links by cross connecting them at optical OXC will result in reliable optical paths that can be used to carry data with the required QoS requirements (e.g., 10^{-12} bit error rate). Indeed, without relying on O-E-O conversion at switching nodes, it is a difficult problem to connect optical channels with the firm guarantee of immediate quality in WDM networks.

This is why in this thesis, we support pre-configuration and fully pre-cross connection of protection capacity in order to provide reliable backup paths and fast service recovery in WDM networks.

CHAPTER 3

Background on Optical Network Survivability

Communication services are taking a paramount place in our social and business daily lives. Our dependence on them has been accentuated by the increasing number of domains where they have been introduced and taking an important role. For example, telephone services serve as a distance transcendent communication and their interruption, even temporary, can cause a social turmoil and business losses. Indeed, in some businesses, disruption of a communication service can suspend critical operations. This in turn, can lead to significant revenue losses for the customer, which are reclaimed from the service provider. Guaranteed availability is one of the important clauses of Service Level Agreements (SLAs) between customers and service providers. An SLA can include stringent constraints regarding different service requirements, and include compensations if they are not met. Though, service interruption is detrimental to both customers and service providers.

Several communication services are supported through different telecommunication network facilities whose reliability is necessary in order to provide reliable services. Communication networks are prone to a wide variety of failures, usually caused by natural disasters (earthquakes, fires, and floods) [Bal96], software bugs [Gry04], and human errors [Kuh97]. Though, survivability against failures is an important feature in many telecommunication networks, but it is a critical issue in high-bandwidth WDM optical networks. Because a large number of high-capacity channels are multiplexed on a single fiber optic and the number of customers that can be affected by a failure is extremely high.

There are a variety of recovery mechanisms used in building protection schemes in survivable optical networks. The main differences between those mechanisms are the required amount of spare capacity and equipment, the recovery speed, the operational complexity, and the number of simultaneous failures that can be recovered. It is common to use a combination of protection mechanisms in order to provide protection with different guarantees, and effectively accommodate as many customers as possible. For example, some demands may have stringent requirements regarding the recovery delay (e.g., less than 50ms), and others high service availability (e.g., 99.999%, or less than 5 minutes/year of unavailability).

In this chapter, we briefly review the state of the art in survivability in optical networks by first introducing some vocabulary and concepts. Next, we review existing survivability mechanisms in optical WDM networks. A particular attention is attached to recovery mechanisms, which provide differentiated quality-of-recovery and quality-of-protection.

3.1 Basic Concepts

3.1.1 Optical Network Failures

Fiber cuts are considered to be the most common failures in fiber-optic networks. One of the reasons why underground fibers are susceptible to failure is due to the fact that they are buried in the same public right-of-ways as other transport utilities (water and gas pipes, television cables). This increases working activities (digging, construction work) around the fibers and their susceptibility to failure. Typically, and not a long time ago, a cable cut happened every 50 to 200 days per 1000 km of cable [MCL+03, BDH+00, WAPD01]. In addition to cable cuts, switching node failures are not unusual and can be more harmful than fiber link failures. Because a node failure can involve more fiber links. though, carry more traffic than a fiber link (see [MCL+03, WAPD01] for typical failure frequency of SONET DXC, WDM OXC. and (O)ADM node equipment).

3.1.2 Reliability and Availability

Reliability of a network element (e.g., a link, a node) is defined as the probability that it will be found fully operational during a certain time frame [ITR94]. Though, the reliability of a component accounts for the time that it will take to fail while it is operating, and does not reflect how long it will take to get the component under repair back into working condition. Reliability of network-components are usually estimated by their manufacturer based on experiments. *Availability* is the instantaneous part of reliability, i.e., the probability that a system is operating properly when it is requested for use at a given time. Though, the availability of a given system is equal to the probability that the system is not failed or undergoing a repair action. In other words, the percentage of time the system is operational. It is usually noted A, and defined as follows [Col87]:

$$\begin{aligned} A &= \frac{Up - Time}{Up - Time + Down - Time} \\ &= \frac{MTBF}{MTBF + MTTR} \end{aligned}$$

where

MTBF: Mean Time Between two Failures.

MTTR: Mean Time To Repair.

The MTTR is a generic term, and it includes all the time intervals during which the service is not available including the restoration time. Typical MTBF and MTTR values in optical networks can be found in [MCL$^+$03, BDH$^+$00, WAPD01, JM98].

3.1.3 Shared Risk Group

A shared risk group is a set of components (e.g., fiber links, switching nodes) that share the same risk of failures. This concept is closely related to the concept of routing diversity. Two lightpaths, routed through a set of nodes and links, are said node/link disjoint if they do not share any common node/link. However, to insure that there is no shared risk group of failures, the lightpaths have to be not only routed through different fibers, but also through different underlying ducts. An example of Shared Risk Link Groups (SRLGs) created by routing different fiber links through shared ducts are illustrated in Figure 3.1. Links $1-4$ and $1-2$ share a routing tunnel along a portion of their length, though the shared risk link group $SRLG_1$. Another $SRLG_2$ appears at the bottom of the figure which includes links $1-4$ and $3-4$.

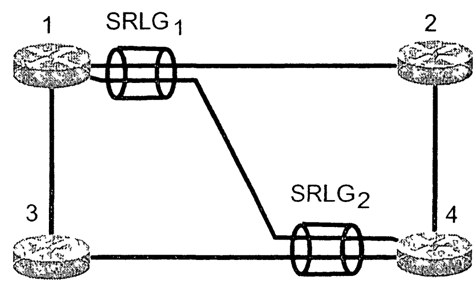


Figure 3.1: Shared Risk Link Group

In Figure 3.1, the physical routing of some optical links differs from their logical routing counterparts. Physical routing of links is usually dictated by different external constraints, e g., sharing existing pipelines in cities or minimizing design costs.

3.1.4 Capacity Redundancy

Before defining the capacity redundancy, we need to define its two associated capacities: Working and spare capacity. Working capacity is defined as the bandwidth used to carry traffic in the nominal situation, i.e., no failure. Spare capacity is the bandwidth reserved for recovery in case of a failure. The spare capacity redundancy, which is the inverse of capacity efficient, is defined by the ratio of the whole spare capacity over the whole working capacity. The required amount of spare capacity in order to provide protection in case of a failure is an important parameter in the design of effective recovery schemes.

3.2 Recovery Mechanisms in Optical Networks

As to limit the interruption time of communication services, most modern telecommunication operators use so-called *recovery mechanisms.* These mechanisms are used in case of a network failure to divert the affected optical lightpaths to protection paths (failure disjoint) in the network.

Figure 3.2 illustrates the basic principle of the recovery process under single-link failure scenario. The *working* path (also known as *primary* path) and the *recovery* paths (also known as secondary or backup path) are node and link disjoint, i.e , they do not share any link or node Though, no single link or node failure in the network, except nodes S and D, can affect both of them. Under

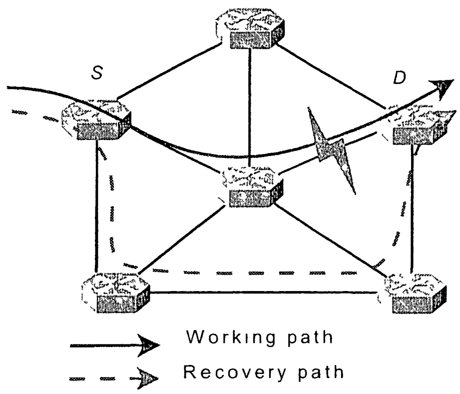


Figure 3.2: Principe of Recovery Scheme

normal conditions (i.e., no failure), traffic from S to D is carried along the working path In case of a failure, e.g., link failure as illustrated in Figure 3.2, the recovery scheme activates the protection path and then switches the traffic onto the protection path.

The recovery process in Figure 3.2 is a generic scheme. Different aspects and functionalities characterize a recovery scheme, e.g., the protected and protection entities, the recovery process, and the underlying technology. For example, based on the protected entities, e.g., links, segments, or paths, three classes of recovery schemes can be formed: link, segment, or path protection. Each of these schemes has its own recovery mechanism and can be managed at the optical layer as well as at other upper layers.

3.2.1 Recovery Cycle

Although a variety of recovery schemes exists, they all operate according to the same recovery cycle [SH03], as illustrated in Figure 3.3. In case of a failure in the network, it takes a time before the

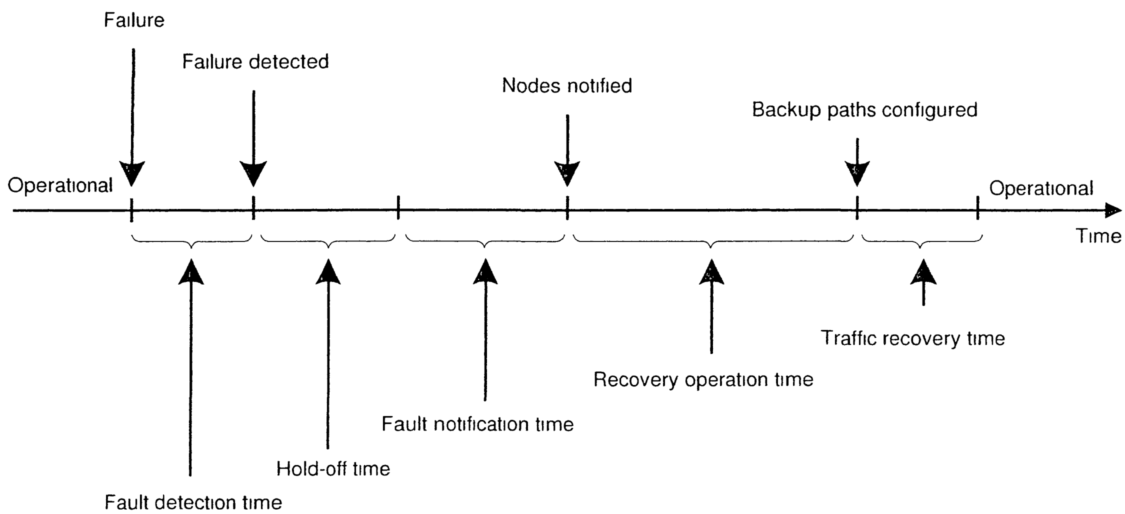


Figure 3.3: Recovery Cycle

adjacent nodes of the failed component find out about the failure. This time depends, for example, on the signal propagation delay, on the speed of the physical layer in failure monitoring, detection, and signaling to the upper layers Once the failure is detected, the node that detected the failure may wait for a hold-off time in order, for example, to allow failure recovery coordination among layers. For instance, in an IP-over-optical network, a hold-off time may be observed by the IP layer in order to give a chance to the optical layer to recover from the failure. After a hold-off time. if the failure still exists, the adjacent node to the failure starts sending notification messages to selected nodes that will be involved in the recovery process. Next, and during the *recovery operation time*. the notified nodes set up the backup path. This time interval may include routing state information exchange, signaling, routing, and management operations. However, these operations are not all necessary if the backup path is pre-configured ahead of failures In fully pre-cross connected protection schemes, where protection paths are set up ahead of any failure at all involved switching nodes (see Section 3.5.1), these two last steps are performed ahead of any failure, though not included in the recovery cycle. After the last recovery operation, the traffic starts to use the backup protection path.

3.2.2 Protection and Recovery Parameters

Depending on the underlying technology, the targeted availability, the supported users and applications, and many other considerations, a variety of protection schemes exist to meet different recovery requirements. In building protection schemes, a trade-off has to be found among different protection parameters including the recovery time, spare capacity requirements, and management and signaling complexity. In the next section we elaborate further on those parameters, and on protection schemes taking into account those parameters.

Recovery Time

As illustrated in Figure 3.3, recovery time is the whole time it takes between a network failure appearance and the time the traffic flows on the backup protection path. In addition to providing protection, the recovery time is the design objective of several protection schemes. Typically, the shorter the recovery delay, the higher is the network availability. In fully pre-configured and pre-cross connected protection schemes the protection capacity is deployed and pre-cross connected, respectively, ahead of any failure. Though, the recovery delay, in case of a failure, resumes to a limited signaling and switching of the traffic onto the backup path. On the opposite side, recovery schemes based on dynamic restoration involve the longest recovery delay. Indeed, dynamic restoration usually includes a link-disjoint path calculation (in path protection), protection capacity establishment. i.e , reservation/confirmation, and switching of traffic.

Backup Capacity Cost

The required amount of protection capacity (backup capacity budget) to protect against some network failures is an important parameter in the design of effective protection schemes. This parameter defines the protection scheme cost. The backup capacity requirement of protection schemes may depend on the shape of the protection building blocks. e g., linear paths. rings, trees. In order to minimize the backup capacity requirement to provide a specific protection level, sharing of the protection capacity among disjoint failure working paths is the most used mechanism [OZZ+04, THV+08, XXQ03, HM02].

Recovery Scope

One of the characteristics of a recovery scheme is its recovery scope. A recovery scheme can be designed to recover from specific failure scenarios, e.g., single, dual, or multiple link or node failures. The recovery scope is usually decided based on the targeted availability. A high network availability may require recovery mechanisms to recover from a wider range of potential failures.

State Overhead

As the protection topology grows (protection paths) and advanced protection capacity sharing mechanisms are used, the amount of state information (overhead) required to accurately maintain the protection topology (e.g., sharability of protection links among working paths. backup capacity availability) also grows. In shared capacity protection schemes, in addition to the availability of the protection resources and the working-protection relationship, failure-disjointness of working paths is an important information in order to maintain an accurate state information regarding sharing of protection capacity. This parameter is used as a criterion to assess the scalability of different recovery schemes.

Signaling Requirements

This parameter is related to the recovery delay. Some recovery schemes may require more protection signaling than others, for instance, in failure notification and recovery, though, involve longer recovery times (see Figure 3.3). Recovery schemes involving high signaling require more resources (CPU time. bandwidth). and more management overheads. The signaling requirement is another criterion used to assess the performance and scalability of recovery schemes.

Stability

Dynamic and reconfigurable recovery schemes involve reconfiguration of the protection topology in order to provide protection against different failure scenarios. Though, they are usually more flexible and cost effective over static schemes. However, and as seen in Section 2.4, dynamic reconfiguration of a lightpath does not necessarily guarantee its integrity, e.g., $BER \leq 10^{-12}$, within a specific time interval, especially in photonic networks.

Recovery Classes

In some recovery schemes, it is possible to provide different guarantees (classes) of recovery for different classes of traffic with different recovery requirements [SGZ04] This is a useful feature, because not all the users need the same guarantees, and not all are ready to pay for the associated prices. Though, recovery differentiation is another important parameter to judge the performance of a recovery scheme.

Protection Classes

Like recovery classes, providing different protection classes is a feature that enables a single protection scheme to survive different failure scenarios based on the user and traffic profiles [OM04, GS02, XCT03]. For instance, providing an availability equal to 98.99% through a protection scheme that guarantees 100% single link failure protection, and an availability equal to 99.99% through a protection scheme that guarantees 100% single link and 80% dual link failure protection. Though, protection schemes providing different protection classes are suited in order to effectively accommodate many types of users and applications.

3.3 Protection Techniques

Protection mechanisms can be implemented in the optical layer, or any other logical layer. e.g., SONET/SDH, IP, ETHERNET, or MPLS [VPD04]. Any network layer, capable of reconfiguring the logical protection topology, for instance, wavelength routed WDM layer, SONET/SDH layer, or IP layer, can provide network protection. Indeed, it is solely required to have a working path and a backup path, which should be failure-disjoint, in order to provide protection at any specific layer. Upon a failure, a recovery process is initiated to activate the backup path at its associated layer. Different layers have different types of technologies, though different switching techniques (e.g., SONET/SDH) and switched entities (e g., wavelength).

The protection technique in the optical layer is usually *link-oriented.* Examples or link-based protection schemes include Automatic Protection Switching (APS), Unidirectional Path-Switched Ring (UPSR), Bidirectional Line-Switched Ring (BLSR), generalized loop-back networks [MBF+02], *p*-cycles [GS98], and pre-configured trails [CCF04a]. These protection schemes involve pre-configuration of the backup paths and usually pre-cross connection of switching nodes ahead of failures.

The protection technique in the logical layer is very often *path-oriented* and *segment-oriented.* Examples of path and segment protection schemes include Shared Backup Path Protection (SBPP) [NBWS04], Shared Backup Segment Protection (SBSP) [XXQ03], and flow *p*-cycle [GS03]. In these protection schemes, failure detection and failure notification are usually performed at the two failure adjacent-nodes, but traffic switching at the two end-nodes of the protected entities, i.e., source and destination of a working path in SBPP, and upstream and downstream nodes of a working segment in SBSP. These schemes have the advantage of spare capacity efficiency over the link protection schemes [RSM03]. However, very often, they require longer recover times and more complex recovery operations. Indeed, the backup path/segment is not necessary pre-deployed, i.e., it is either pre-computed, but only reserved after a failure, or reserved but only configured in case of a failure. This in turn, will necessitate a signaling process to reserve the backup path/segment. and to set up the switches along the backup path/segment.

Although each of the higher layers may have its own protection and restoration mechanism. it is highly attractive to provide protection at the optical layer for the following reasons [GR00a. GR00b, GRS98. CLB98]:

- Speed: Recovery at the optical layer is much faster because the nodes can act quickly upon the occurrence of failures and do not wait for upper-layer signaling.

- Simplicity: It needs less coordination, less management and signaling overheads than recovery at higher layers. This is due to the number of protected entities in the optical and logical layers, i.e., a few wavelengths vs. millions of connections.

- Effectiveness: Protection at the optical layer makes a more efficient use of protection capacity because of resource sharing among different service layers.

- Transparency: The wavelength protection technique is independent of the protocols and applications used in the higher layers.

3.3.1 Automatic Protection Switching Technique

Automatic Protection Switching (APS) is typically used to handle link failures in the optical layer. It has three main architectures: $1 + 1$, $1 : 1$, and $1 : N$ [Wu92]. Figure 3.4 illustrates these three protection architectures. In $1 + 1$ APS, each working link is provided protection by a parallel backup

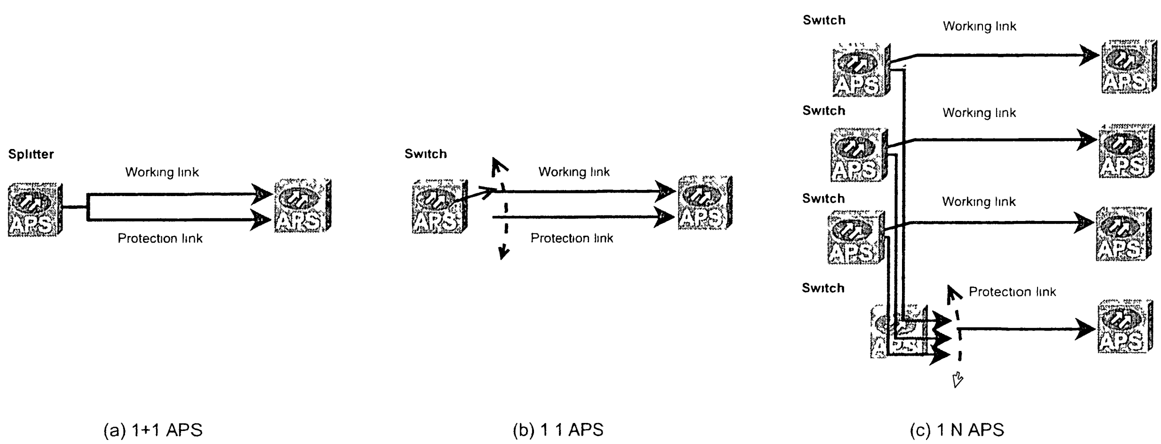


Figure 3.4: Automatic Protection Switch

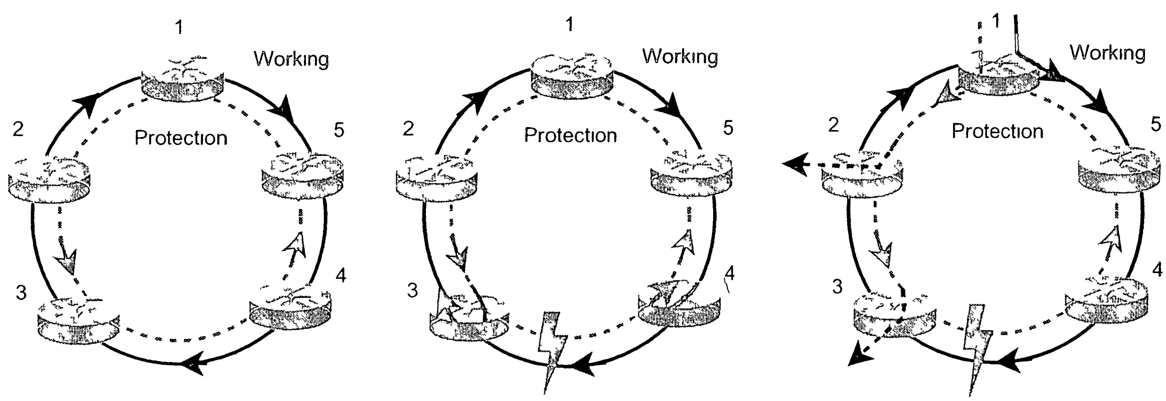
link. At the source node, the signal is launched on both the working and backup links. The receiver at the destination node compares the two signals and chooses the best one (e.g. BER $\leq 10^{-12}$). With such an architecture, if one link fails, the destination node is still able to receive the signal on the other link. In 1:1 APS, the source and destination nodes switch to the protection link only when a failure on the working link is detected. Under normal operations, the protection link is either idle or used to carry low-priority traffic. In $1 : N$ architecture, N failure disjoint working links share a single protection link However, unlike in 1 1 APS, in order to guarantee 100% single link protection, the traffic switched to the protection link must be switched back to the working link after it is repaired In general, an M N APS protection refers to a scheme in which M protection links are shared among N working links This generic scheme can survive $\min\{M, N\}$ simultaneous link failures

3.3.2 Self-Healing Ring Technique

In a ring network, the working and protection logical topologies are restricted by the physical topology of the network The ring protection technique is more flexible than APS because it can handle both link and node failures The development of high speed add/drop multiplexing (ADM) technology has simplified protection switching and made SHR a very attractive approach to provide survivability Unidirectional SHR (USHR) and bidirectional SHR (BSHR) are two types of SHRs techniques

Unidirectional Self-Healing Ring (USHR)

Figure 3 5 (a) shows a USHR architecture In USHR, the logical ring topology carrying normal traffic goes around the ring physical topology in one direction In case of a failure, the working traffic is switched onto the logical ring topology in the opposite direction USHR protection can



(a) USHR (b) Line protection USHR (c) Path protection USHR

Figure 3 5 Unidirectional Ring Protection Technique

be performed in two different ways Line protection switched USHR and path protection switched

USHR. In line switched USHR, as illustrated in 3.5-(b), it is up to the two failure-adjacent nodes to switch the affected traffic onto the protection ring. Therein, a failure on a link (two fibers) between, e.g., nodes 2 and 3, is recovered from at node 4 by switching the traffic onto the protection fiber, and at node 3 by switching the traffic back from the protection to the working fiber. This architecture can also survive any node failure.

Path protection switched USHR is basically a 1 + 1 protection scheme because the optical signals are transmitted on both fiber rings. A link failure in this case cannot affect both the working and protection fibers. Though, the destination node monitors the two signals and chooses the best. As shown in 3.5-(c), the link cut between nodes 2 and 3 will affect all the traffic toward node 3 on the working ring, but not on the reverse protection ring. Thus, node 3 will choose those signals transmitted toward it on the protection ring as the best signals. As no signaling or dynamic switching is required, path protection switched USHR is considered the fastest SHR scheme.

Bidirectional Self-Healing Ring (BSHR)

Unlike UPSR, in BSHR, working traffic flows in both directions. The typical architectures of BSHR are two- and four-fiber line protection BSHR/2 and BSHR/4. In BSHR/2, as shown in Figure 3.6-

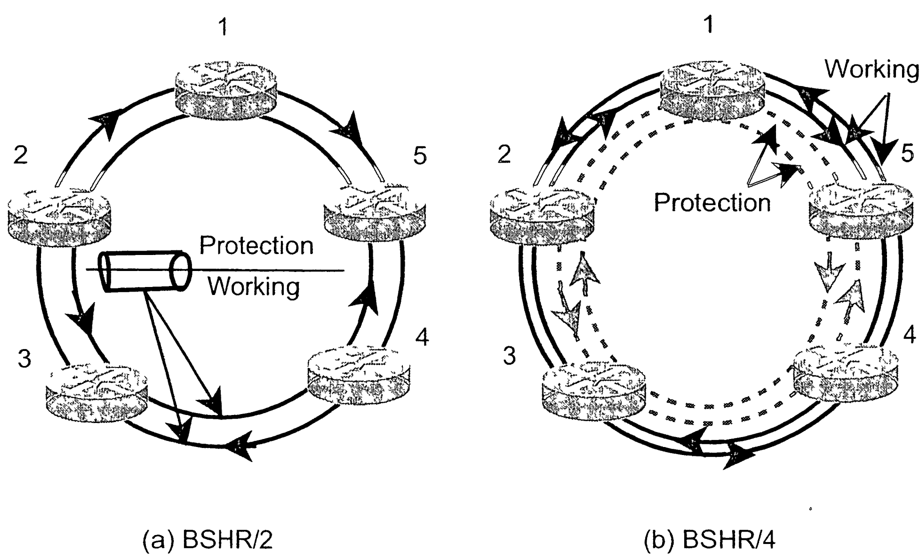


Figure 3.6: Bidirectional Ring Protection Technique

(a), half of the total capacity on each ring is reserved for protection. As a line switched approach, when a failure occurs, the two nodes adjacent to the failed component will loop the affected traffic using the reserved capacity on both rings. In BSHR/4, as shown in Figure 3.6-(b), two fibers are dedicated as working fibers, so the capacity on them can be completely utilized. Upon a failure, the nodes adjacent to the affected component will simply switch the affected traffic onto the protection fibers.

The evolution of communication traffic patterns has greatly re-shaped the physical topology of modern telecommunication networks, which has led to mesh topologies. Protection in mesh networks is usually more complicated than point-to-point APS or ring networks. To re-use the simple and easy recovery mechanism of rings in mesh networks, there has been a proposition to directly deploy protection rings in mesh networks [SGM93]. In this approach, called ring cover, a set of rings that covers every link in the mesh at least once is found. However, the major drawback of this solution is its capacity redundancy, i.e., need for a large amount of spare capacity to get 100% protection guarantee [EHS00].

3.3.3 Mesh-Based Technique

Mesh topologies using optical cross-connects (OXCs) have started to emerge with the extensive deployments of WDM systems. Design of protection schemes in mesh topologies is more challenging than in ring topologies. as it involves hard combinatorial problems, especially, when the network size and connectivity increase. The most studied protection parameter and failure scenario in the design of protection schemes in survivable WDM mesh networks have been protection redundancy and single-link failures, respectively. Proposed solutions for efficient use of protection capacity fall under two categories: protection and dynamic restoration. Dynamic restoration involves reservation of protection capacity only in case of a failure, though, no spare capacity is pre-reserved. However, dynamic restoration is usually complex, i.e.. requires up-to-date state information and extensive signaling. and its restoration time is much longer than protection. In addition. and as seen in Section 2.4. from the engineering point of view. engineering of an end-to-end backup path requires a delay before it can achieve a specific signal quality (e.g., $BER \leq 10^{-12}$).

Protection is by far the most studied resiliency approach in WDM optical mesh networks. In order to provide protection against single-link failures, we will present in the next sections the three proposed pre-configured protection approaches: Link based protection, path-based protection, and segment-based protection.

Link-Based Protection

In link-based protection, a backup path is reserved for each working link. In case of a link failure, traffic is rerouted around the failure by using a backup path associated to the working link. As an example, in Figure 3.7-(a), in case of a link failure between nodes 3 and 4. the affected traffic will be rerouted around the backup path $3-1-4$. Here, nodes 3 and 4, i.e., end-nodes of the failed link,

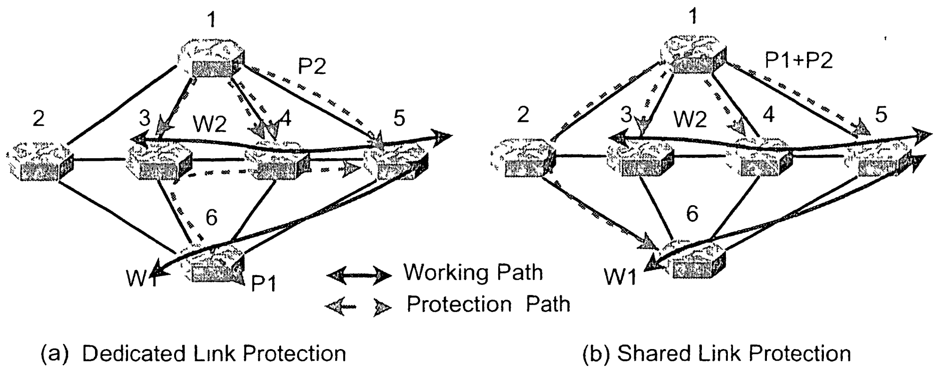


Figure 3.7: Link Protection Scheme

are responsible for traffic recovery. However, as protection capacity is reserved, recovery in this case is limited to end-to-end protection capacity configuration and traffic switching. In link protection, and in order to correctly switch the traffic in case of a failure, each switching node needs to maintain at least a local representation of the protection topology (a local routing database of the protection topology), and be able to perform failure monitoring and detection.

Link-based protection schemes can be further classified as dedicated or shared link protection. Dedicated link protection means that a protection channel (wavelength) path is exclusively reserved to protect each working channel link Therefore, if two protection paths of two different working links overlap at some links. then, different wavelengths must be assigned to them on the overlapping links As an example, consider Figure 3.7-(a). The illustrated working path $3-4-5$ is provided link protection by the backup paths $3-1-4$ for link $3-4$, and $4-1-5$ for link $4-5$. These two backup paths overlap on link $1-4$, thus, two different wavelengths, say λ_1 and λ_2, are allocated to protect the two working links. The main drawback of dedicated protection, particularly dedicated link protection, is its protection capacity inefficiency. Indeed, in Figure 3.7-(a), six backup channels are required to protect only three working channels, which makes the scheme 200% capacity redundant. On the other hand, dedicated link protection may offer protection against failures of multiple links. For example, in Figure 3.7-(a) 100% protection is guaranted even when all working links fail simultaneously.

Shared link protection allows different protection paths to share a backup wavelength on common links if the corresponding protected working channels are failure-disjoint, i.e., link or node disjoint. Figure 3.7-(b) shows an example of a shared link protection scheme. Protection paths $6-2-1-5$ and $4-1-5$ (used to protect working channels on links $6-5$ and $4-5$, respectively) are sharing a wavelength channel on link $1-5$. In case of a link failure, a dynamic mapping of the protection links is required at node 1 in order to isolate (set up) the appropriate backup path. Though, more signaling is required and larger state information is needed than in dedicated protection.

Path-Based Protection

Path-based protection refers to the reservation of a protection path, failure-disjoint with the working path it protects, for each end-to-end working path. In contrast to link-based protection, where only the two end-nodes of a protected link that are involved in the recovery process (monitoring and traffic switching), in the path-based protection more switching nodes are involved in the recovery process. Indeed. failure monitoring and notification are performed at intermediate nodes of the backup paths, and backup path signaling and switching are initiated at the end-nodes of failing paths. Indeed, upon failure of a link, the adjacent-nodes to the failing link notify the source and destination of all involved wavelength-paths, which in turn, activates their corresponding backup paths and then switches the traffic.

Similar to link-based protection, path-based protection can be dedicated or shared. In dedicated

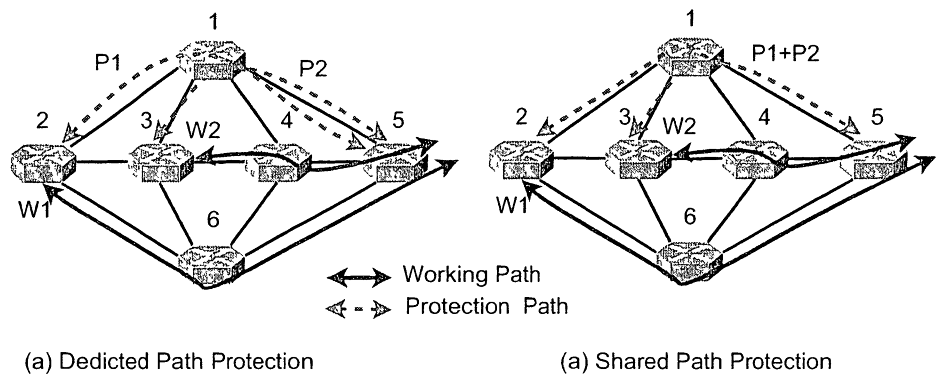


Figure 3.8: Path Protection Scheme

path protection, a backup path is exclusively reserved for each end-to-end working path. In this case, like in link protection, overlapping protection paths use different wavelengths, even if the working paths are link/node-disjoint For example, Figure 3.8-(a) shows two link/node disjoint working paths, $W_1 = 2 - 6 - 5$ and $W_2 = 3 - 4 - 5$ protected by $P_1 = 2 - 1 - 5$ and $P_2 = 3 - 1 - 5$. respectively. The two protection paths overlap on link $1 - 5$. However, because they are dedicated protection paths, they are allocated each a different wavelength on link $1 - 5$. The positive aspect of dedicated path protection is that it enables recovery not only from single-link failures, but also from some multi-component failures, e.g., multi-link and multi-node failures. However, as a dedicated approach, it requires larger protection capacity compared to shared protection.

Shared path protection allows the use of the same wavelength on a shared-link if the protected working paths are link-disjoint. Thus, it results in a more efficient use of the protection capacity. An example of shared path protection is illustrated in Figure 3.8-(b) where the two previous protection paths P_1 and P_2 share the same wavelength on link $1 - 5$.

Regarding the recovery delay, it is different whether the protection is dedicated or shared. In dedicated protection, the end-to-end backup path can be set up at all intermediate nodes before any failure. In case of a failure, the two end-nodes of the affected paths will only need to switch the traffic onto the backup paths when they receive the failure notification In shared protection. depending on the configuration of the protection capacity. re-configurations at intermediate nodes may be required in order to isolate (set up) a backup path. In Figure 3 8-(b). a dynamic switching will be required at node 1 in order to isolate any of the two backup paths: connect either link $2 - 1$

or $3 - 1$ to link $1 - 5$.

In the design of protection schemes, there is a clear trade-off between the capacity cost and the recovery delay. The comparison between link and path protections, shows that path protection is more capacity efficient than link protection, but in terms of recovery delay, link protection achieves faster recovery delay and requires less management and signaling overheads [RM99].

Segment-Based Protection

Segment protection can be seen as a compromise between link-based and path-based protection techniques. Indeed, the basic protected entity is a segment, which is usually shorter than an end-to-end path, and longer than a single hop link. Examples of segment protection schemes include Shared Backup Segment Protection (SBSP) [HM04, THV+08, XXQ02, SG04a, XXQ03], and flow p-cycles [SG03c, SG03b].

Figure 3.9 illustrates a segment protection scheme. The overlapping protection segments $2 - 1 - 4$ and $3 - 6 - 5$ provide 100% protection against any single link or node failure. In case of a link failure,

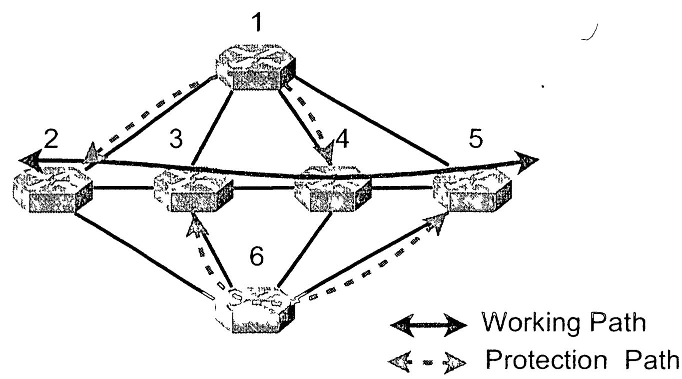


Figure 3.9: Segment Protection Scheme

a notification will be sent to the upstream and downstream of the affected working segments, which in turn, initiate the recovery process. Recall that protection segments can also be non overlapping, in which case, they lose their node protection capability. Compared to path protection, segment protection can provide faster recovery delay because recovery is performed at intermediate nodes, which are usually not far from the failure location. Regarding capacity efficiency, shared segment protection achieves better capacity efficiency than shared link protection [XXQ02].

3.4 Multi Layer Protection

So far, we have only discussed protection techniques to provide recovery in case of a failure at one network layer (technology). However, in a realistic multi layer network, recovery is usually carried simultaneously at different layers. For instance, in an IP over OTN architectures, IP restoration could be used to recover from IP router failures, and point-to-point optical protection could be used to recover from fiber link failures.

Some of the high-layer services, such as SONET and ATM, have their own protection mechanisms, and some others have no recovery mechanisms incorporated in their layers. The optical layer protection, although highly efficient against failures in the optical layer, cannot protect against failures at higher layers. In order to provide protection against failures at the high-layers, additional recovery mechanisms must be implemented at those layers as well. Integration of recovery mechanisms at multiple layers raises the issues of assigning recovery functions to each layer and coordinating the whole recovery process. Based at which layer the recovery process is initiated. and the interaction between the different layers, a set of rules, named *escalation strategies* [Dem99], have been proposed in order to coordinate the multi-layer recovery operations. Based on the layer at which the fault recovery process is initiated, two escalation strategies have been proposed in [Dem99]: the bottom-up strategy and top-down strategy. These strategies have a common feature which resides in the fact that a fault is never resolved in different layers at the same time. To achieve this, a chronological recovery order is imposed for the different layers, and a set of racing recovery conditions is defined in order to coordinate the multi-layer recovery operations. The chronological order of recovery at the different layers can be established through a hold-off timer (see Figure 3.3).

In the bottom-up strategy, recovery starts at the optical layer, and escalates upward upon expiration of the hold-off timer. For instance, in case of a failure in the optical layer, the recovery process can be started in the optical layer immediately, whereas the logical layer (e.g., IP layer) observes a hold-off time before initiating its recovery process. If the failure is recovered in the optical layer before the hold-off timer expires, the upper layer will not initiate a logical layer recovery. In the top-down strategy, recovery always starts at the uppermost client layer and escalates downward.

The disadvantage of this approach is the potentially large number of traffic streams that must be restored at the logical layers.

3.5 Pre-configured Protection Structures

The performance of a protection scheme in providing recovery in survivable optical WDM networks depends greatly on the shape of its logical protection topologies. In mesh WDM networks, protection schemes are built by a combination of a variety of wavelength protection topologies including, for example, rings, cycles, linear paths, trees, stars. Individually considered, each of these pre-configured protection topologies is characterized by some protection parameters including, for example, its protection capacity budget (cost), protection capability, recovery speed, required management and signaling overheads, and ability to survive single and multiple failures.

Different protection blocks (logical topologies), ranging from simple linear paths to highly-connected topologies, can be used to provide protection in survivable WDM mesh networks. Contrary to ring topologies, mesh topologies enable advanced protection structures, though, efficient sharing of the protection capacity. In this section, we review some design approaches of link-based protection using pre-defined shape protection structures, and study their advantages and disadvantages. We focus more on the degree of pre-configuration of the protection structures. and discuss their recovery delays and protection capacity costs.

3.5.1 Fully Pre-Cross Connected Schemes

The concept of pre-cross connected protection extends the pre-configuration of protection capacity from backup capacity reservation to end-to-end setup of the protection paths, i.e., backup capacity is reserved and switched or cross-connected at all optical nodes along the backup paths. This feature is very important, especially in photonic and translucent networks, in order to optimize the CAPital and OPerational EXpenditures (respectively CAPEX and OPEX). Indeed, not all signals need to be dropped at all intermediate nodes along their way to destination. Bypassing some signals coming along some ports can help in saving on transponder costs. power. and reduces the vulnerability of the switching nodes. Above all, pre-cross connectivity guarantees reliable end-to-end backup paths ahead of failures, i.e., backup paths are guaranteed to be in a good condition before their use. Examples of pre-cross connected structures include pre-cross conencted cycles (p-cycle) [GS98] and pre-cross connected trails (p-trails) [CCF04a].

The p-cycle based approach is an extension of the self healing ring protection. Like any cyclical structure, a p-cycle can achieve high recovery speed in case of a failure. Indeed, in case of a link failure, only the two end-nodes of the affected link will need to switch the affected traffic onto the backup path (see Figure 3.10). Intermediate nodes will only pass the traffic without any reconfiguration of the protection capacity. Unlike a shared ring structure, which is at least 100% redundant, a p-cycle can protect larger capacity, and thus, is less redundant than a ring structure. Figure 3.10 shows a unit capacity p-cycle providing 100% single-link protection within the illustrated

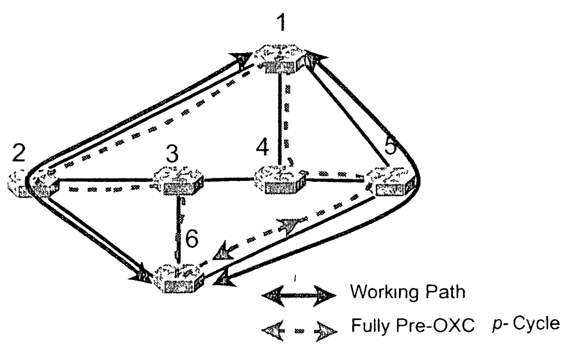


Figure 3.10: Fully Pre-Cross Connected Cycle p-cycle

working plane (one wavelength working paths). The working traffic carried on links that are also spanned by the p-cycle (called on-cycle links, e.g., $1-2$ and $5-6$) is protected by switching the working capacity onto the protection cycle all around the affected link; while on-cycle links whose end-nodes are also spanned by the p-cycle, but not the links. (called straddling-cycle links, e.g., $1-5$ and $2-6$) are protected by switching the working capacity either on one of the two backup paths offered around the p-cycle.

The recovery speed of p-cycle and ring based protection schemes is not really due to their logical topology. Rather. it is due to the fact that there is a unique way to map incident protection wavelength links at switching nodes. Indeed. there is either zero or two links of the p-cycle incident at switching nodes. Though, they can be pre-cross connected ahead of failures in a deterministic way, and used without reconfiguration in case of a failure

The p-trail is a linear protection structure that can be shared and fully pre-cross connected ahead of any link failure too. As in the p-cycle approach, there is no need to re-configure any cross connect along the backup path in order to provide 100% protection. Figure 3.11 show two p-trail structures providing protection within the same previous working plane. Although this approach is

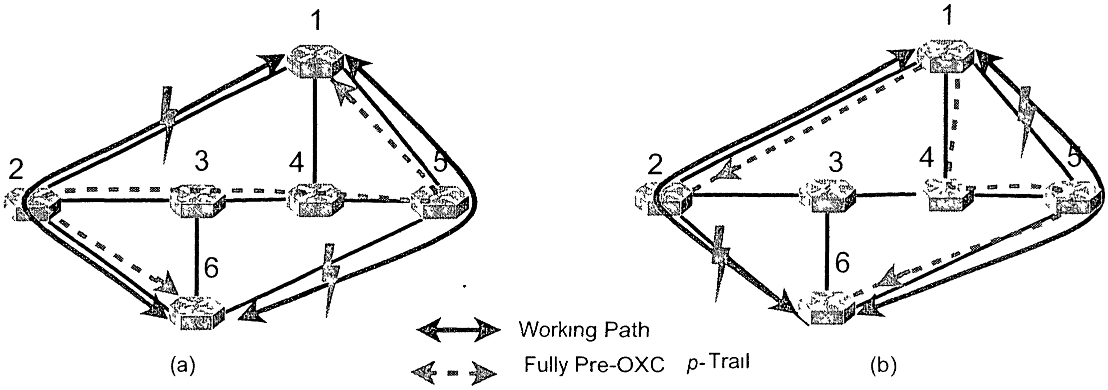


Figure 3.11: Fully Pre-Cross Connected Trail p-Trail

less capacity efficient than the p-cycle one, it has an advantage over the p-cycle when it comes to deployment in sparse and constrained link spare capacity budget.

In fully pre-cross connected structures, the recovery process following a link failure involves almost all the overlay protection structure, e.g., a failure of link $1-2$ in Figure 3.10, or link $2-6$ in Figure 3.11-(b). Such a protection feature, raises a vulnerability issue to dual and multiple failures in the network.

3.5.2 Dynamically Cross Connected Schemes

In fully pre-cross connected schemes, the protection capacity is allocated following a pre-defined plan which enables protection structures to be fully pre-cross connected ahead any failure. However, this additional constraint, may induce an extra protection capacity cost in order to provide the same protection level. Figure 3 12 shows a pre-configured protection structure. a spanning p-tree, where there is no pre-cross connection of the protection capacity at any switching node

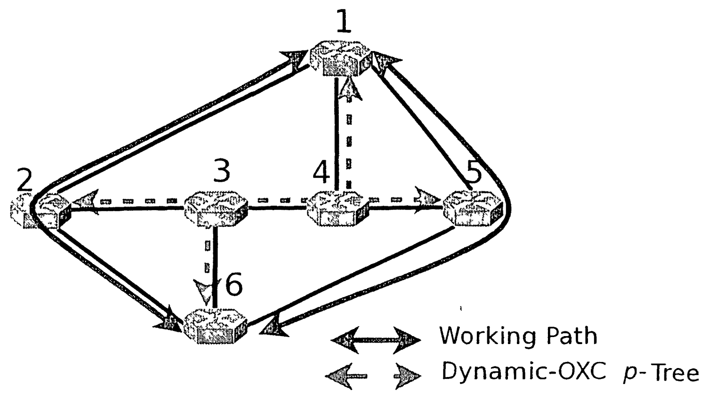


Figure 3.12: Dynamically Cross Connected Structure

In this scheme, the protection capacity is dynamically cross connected in case of a failure in order to set up any backup path. Though, in case of a failure of any working link, a signaling process will be initiated in order to cross connect the protection capacity at intermediate nodes of protection paths. For instance, in case of a failure of link $1-2$, a dynamic switching will be performed at both node 3 and 4 in order to isolate the backup path $2-3-4-1$. This approach allows high flexible protection capacity allocation, which can be used to meet different protection objectives like cost and resiliency against multiple failures. The illustrated p-tree based scheme in Figure 3.12, requires less protection capacity and it is more resilient against dual-link failures than the previous fully pre-cross connected scheme in providing the same protection and resiliency levels. However, its disadvantage lies in its recovery process. As intermediate nodes need to dynamically change their configuration, this adds to the global recovery delay of the protection scheme.

3.5.3 Partially Pre-Cross Connected Schemes

This approach leads to a compromise between the two previous ones [Sim07] A trade-off between the recovery speed of the fully pre-cross connected structures and the flexibility of the dynamically cross connected ones is sought by this protection approach. In partially pre-cross connected schemes, the number of dynamic cross connections in order to recover from any failure is limited. though. the recovery delay inherent to reconfiguration of the cross connects is limited too. The pre-cross connectivity property has its price in terms of protection capacity, and it is controlled in this approach too.

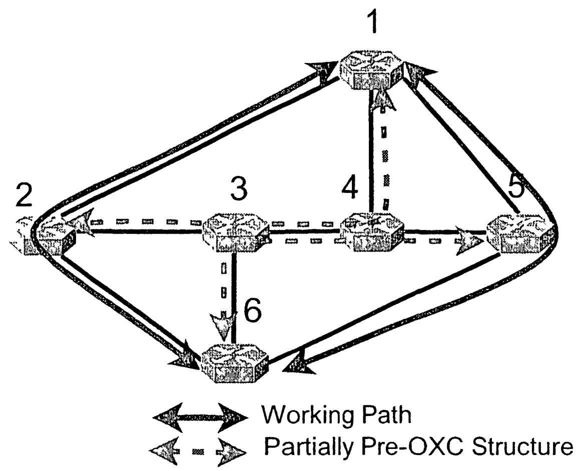


Figure 3.13: Partially Pre-Cross Connected Structure

Figure 3.13 illustrates a partially pre-cross connected protection scheme, which provides protection with the same previous working plane. In this scheme, in order to recover from any link failure, there is a single cross connect at node 3 that needs to be re-configured dynamically. Two different backup channels are used on link $3-4$ in order to avoid dynamic reconfiguration at node 4

In terms of protection capacity budget, partially pre-cross connected schemes require a bit more protection capacity than dynamically cross connected scheme. Two wavelengths are used on link $3-4$ instead of one in the previous dynamically cross connected scheme.

3.6 Summary of Protection Approaches

In Figure 3.14, we represent a summary of protection approaches classified as shared and dedicated protection schemes. The shared protection schemes are, in turn, classified according to their protected entities and to the pre-configuration of their protection topologies (same classification of dedicated protection schemes also exists). A protection scheme is either link, segment, or path oriented depending on the protected entities. Each of these schemes can either be fully or partially pre-cross connected ahead of failures. or dynamically cross connected in case of failures.

Figure 3.15 shows the variation of the capacity redundancy and the recovery delay of the different classes of protection schemes. According to the protected entities. the path protection approach is

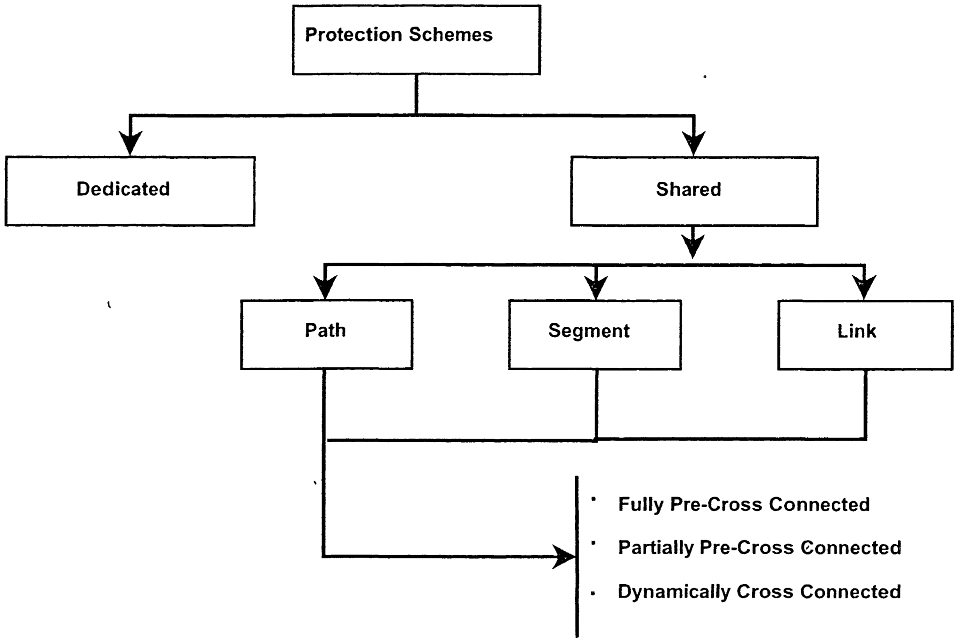


Figure 3.14: Classification of Protection Schemes

known to be more capacity efficient than the segment which is in turn more efficient than the link approach [RSM03, XXQ03]. The recovery delay parameter in this case varies inversely with the capacity redundancy parameter. Indeed, the recovery delay depends on the recovery process, which involves larger signaling overhead and complex operations than in segment and link approaches.

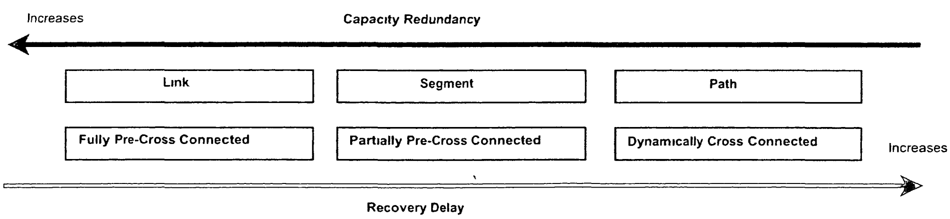


Figure 3.15: Protection Performance: Capacity Redundancy and Recovery Delay

According to the pre-configuration of the protection capacity, the recovery delay of fully pre-cross connected scheme is known to be low [GS98, CCF04a], and it increases as the number of cross connects that need dynamic reconfiguration increases [Sim07]. Regarding the capacity redundancy it varies inversely with the recovery delay [Sim07] (see Chapter 8).

CHAPTER 4

Background on Optimization of Survivable WDM Networks

In the design of large scale systems such as telecommunication networks, there is a fundamental need for efficient and scalable tools in order to perform network design and planning. Over the last decades, telecommunication networks have grown in size and complexity. Network coverage (or reach) limits have been pushed to regions, countries, and even continents, and a variety of technologies have been developed to increase the network capacity. The network physical topology and capacity expansions have increased the challenges related to the design and planning problems in modern telecommunication networks. Nowadays, with the fierce competition in the telecommunication business, network operators are more than ever interested in design and planning strategies that would optimize their deployment and operational budgets while providing different services.

Design of optical networks, particularly survivable WDM networks, involves different parameters and objectives. In survivable WDM networks, design of logical protection topologies has attracted many researchers over the last two decades. Greedy algorithmic and classical Mixed Integer Linear Programming (MILP) based optimization approaches have been widely used in the design and planning of protection planes. However. with the increasing size and complexity of network topologies, the current optimization approaches are not always practical nor effective, especially, in large scale networks. Indeed. efficiency of greedy algorithms and scalability of classical MILP approaches are greatly dependent on the size of the problem inputs and the quality of the targeted solutions.

The prevalent design approach of protection schemes in survivable WDM networks is based on a two-step method [SG04b, SG05, ZZB05, SG03a, RT05]: A first step where. (all/some) potential protection structures, e.g., paths, cycles, trees, to provide protection against different failure scenarios are pre-enumerated, and a second step where selection of the most relevant ones is performed through ILP optimization to meet different objectives. The drawback of such an approach lies in the way the modeling and optimization steps are performed. The number of candidate protection structures grows exponentially as the network size increases, e.g., there could be up to $\binom{M}{3}+\binom{M}{4}+\binom{M}{5}\cdots+\binom{M}{M}$ cycles in a network of M links, and most of them will not be of interest in the final solution. Furthermore, the second step, which is usually based on ILP optimization, takes as an input the output of the first step, though, highly dependent on the size of the candidate protection structure space. This, in turn, affects the scalability and efficiency of the ILP optimization step.

This chapter is dedicated to a review of some mathematical modeling techniques and solution methods to design protection schemes in survivable WDM networks. First, we start by reviewing some graph concepts and algorithms with some of their applications in the design of protection topologies. We focus on algorithms to construct different shape protection topologies and protection design metrics. The concepts of single and multiple link/node and SRLG disjoint protection paths are given a high priority as they are the key issues in several protection scheme design algorithms. Secondly, we review Linear Programming (LP), ILP, and Column Generation (CG) optimization techniques. We emphasis the CG decomposition approach by reviewing its associated modeling and solution techniques.

4.1 Graph Algorithms

A graph is a mathematical concept used to abstract network topologies in communication networks and several other processes in different fields. From now on, we represent a network topology by a graph $G = (\mathcal{V}, \mathcal{L})$ where $\mathcal{V}$ refers to the set of vertices or nodes. and $\mathcal{L}$ to the set of edges or links A link in this thesis refers to a set of physical fibers laid down between two nodes and sharing the same physical duct. Though, a link can be either unidirectional or bidirectional depending on the orientation of the fibers laid down along the link. Sometimes, fibers share some portions of a duct, see Figure 3.1. In such cases, fibers are considered to form different links but share the same risk of failure along the shared portions of the duct.

Next, review some graph algorithms which are widely used in the design and planning of survivable WDM optical networks.

4.1.1 Protection Path Algorithms

Backup path calculation algorithms are very often used in the design of survivable transport networks to enumerate candidate routes as inputs to the optimization problem. In order to provide protection against any type of failures, e.g., node or link failure, the backup and working paths should be failure-disjoint. For example, to survive any single link failure, a backup path and its protected working path should be link-disjoint. The most commonly used link/path-disjoint protection path algorithm belongs to the family of shortest path algorithms [Dij59, Flo62]. A comprehensive reference for shortest path algorithms is presented in [DP84]. A backup path can be node-disjoint, in which case it can provide node protection. There is a trade-off between a backup path length and its protection capability. Shorter paths (in terms of number of hops) tend to minimize the protection cost, but at the same they are less shard than long paths. Though, in practice, backup paths are calculated according to different metrics, not necessarily the shortest paths, such as SRLG-disjoint paths and inter-channel interference minimizing paths.

Another family of algorithms used in the computation of protection paths is the k-shortest paths [Epp99]. In this case, k shortest paths are constructed in order to protect each working entity, e.g., link or path. Such a strategy has been widely used in enumeration of candidate protection paths in several optimization techniques in the literature [PM04]. Although, k shortest paths approach results in larger optimization models, it is usually more efficient than the single backup path for each working path approach in path protection.

In the next section, we review some algorithms to construct some pre-defined shape protection structures different from the simple linear paths.

4.1.2 Protection Structure Algorithms

In this section, and without any restriction, by a protection structure we refer to any shaped structure other than a linear path. Though, cycles, trees, squares,..., which can be physically divided into simple linear paths, are considered as protection structures. The advantage of using such structures rather than simple linear paths resides in the protection cost. Sharing of protection capacity is improved by allowing disjoint protection paths to mutually protect each others. For instance, a p-cycle can protect its on-cycle links, in comparison to its two constituent paths, which can only protect their straddling-path links.

In the design of protection schemes in survivable optical networks, two pre-defined shape protection structures have been extensively used: The pre-configured cycle (p-cycle), and the pre-configured protection tree (p-tree) In prevalent design approach of survivable WDM networks based on pre-defined shape structures, the set of candidate structures is pre-enumerated ahead of the optimization process following a given strategy. However, depending on its size, a transport network may have up to millions or even billions of potential protection structures (e.g., p-trees). In order to limit the number of candidate protection structures, heuristic approaches have been proposed in the literature to scale both the pre-enumeration and the optimization steps [DHGY03. GD02. SHY09. KG05, GG07, TT05]. Those approaches are usually based on some specific design metrics.

Design Metrics

The solution spaces of p-cycles and p-trees increase as the network topology size and connectivity increase. Then, a question arises. *what is a good criterion to select a limited number of structures that may be used to achieve a good solution while minimizing the size of the candidate structure set?*

One of the design metrics used in the design of p-cycles is the Topological Score (TS) [GD02]. The TS of a given p-cycle is the maximum amount of potential working capacity it can protect independently of its required spare capacity. This metric favors large size protection structures which can protect larger capacity (large number of paths), but at the same time require high spare capacity budget. According to this metric, Hamiltonian p-cycles and spanning p-trees (span all nodes) are first enumerated before other smaller p-cycles and p-trees. An alternate metric considering both the protected capacity and the protection capacity, called the a priori efficiency (AE), was proposed in [GD02]. The AE of a given protection structure, e.g., a p-cycle, is equal to the amount of a priori protected capacity over the protection capacity.

Both TS and AE are metrics used in pre-enumeration of candidate structures, though, they only indicate the potential efficiency of the protection structures. The real efficiency of a protection structure and of a given protection scheme depends on the traffic distribution and spare capacity budget. The capacity efficiency of a given protection structure is a function of the traffic it protects, and it differs from the traffic it can potentially protects. Furthermore, the link protection budget, also called link spare capacity budget. can prevent deployment of protection structures on some links, though, affects their TS and AE.

Cycle and Tree Searching

Searching for all simple cycles or trees in a graph is a hard combinatorial problem which involves a huge input solution space. To find all/some protection cycles or trees in a graph, an explicit exploration of all the solution space is usually needed. In this section, we describe cycle and tree searching algorithms that are used to generate these input protection structures.

The most widely used approach in simple-cycle searching is based on a Depth First Search (DFS) research method [DHGY03, GD02, KG05]. The DFS algorithm is a search and label technique that incrementally construction a tree. It is an iterative algorithm that solves the problem by searching all simple cycles passing through a node. Initially, it starts at an arbitrary node v_i by exploring its adjacent nodes $v_t (t \in \mathbb{Z}^+)$ that are not yet labelled. If v_j is not labelled, it is assigned a label that indicates that it has already been explored and cannot be considered within the current DFS starting at v_i. and the DFS repeats the same steps from v_j. This process is repeated until the initial node v_i is encountered again (closed cycle). If at a given node. all its adjacent nodes are already labeled. then the DFS algorithm will simply backtrack to the preceding node from which the current node has been labelled and proceeds with the next unlabelled node. The entire algorithm iterates until there is no unlabelled node adjacent to v_i. Once all adjacent nodes to v_i have been labelled, though, all possible cycles through v_i have been enumerated, the algorithm removes v_i and all its adjacent links, and repeats the previous labeling process from another node v_k in the graph, then, continues until there is only one node left in the graph.

Although, some efforts have been dedicated to p-tree based scheme [MFB99, GCM$^+$03, LYSH03, SHY04, TT05], there has been no efficient algorithm for trees construction and optimization.

4.2 Integer Linear Programming

In this section, we study some modeling and solution methods based on Integer Linear Programming (ILP) techniques. ILP is an optimization technique of a linear objective function, subject to a set of linear equality or inequality constraints and variable integrality constraints [NW99]. ILP modeling and solution techniques can be applied to various fields of study. It is used for solving hard combinatorial problems where polynomial algorithms do not exist or are impossible to elaborate. Industries that use ILP models and solutions include transportation, telecommunications, and manufacturing. In the telecommunication domain, they have been proved useful in modeling and solving a variety of problems in design, routing, scheduling, and assignment in wireless and wired networks.

4.2.1 ILP Modeling

ILP programs can be expressed either in an equation or matrix form. The following two models in equation and matrix forms illustrate a generic ILP model of link protection scheme design based on a pre-defined shape protection structure. Let us suppose that the protection building blocks are p-cycles. Based on a set $\mathcal{S}$ of pre-enumerated p-cycles, this model enables the selection of the most efficient p-cycles among $\mathcal{S}$ according to the stated objective.

Equation form:

$$\text{Minimize} \quad \sum_{s \in \mathcal{S}} c_s \, z_s$$

subject to:

$$\sum_{s \in \mathcal{S}} a_{\ell,s} \, z_s \leq b_\ell \qquad \ell = 1,\ 2,\ 3, \ldots, |\mathcal{L}|,$$

$$z_s \geq 0 \text{ and integers} \qquad s = 1,\ 2,\ 3, \ldots, |\mathcal{S}|.$$

Matrix form:

$$\text{Minimize} \quad (c_1, c_2, c_3, \ldots, c_{|\mathcal{S}|}) \,.\, (z_1, z_2, z_3, \ldots, z_{|\mathcal{S}|})^T$$

Subject to:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & a_{1\ |\mathcal{S}|} \\ a_{2,1} & a_{2,2} & \cdots & \cdots & a_{2.|\mathcal{S}|} \\ \vdots & \vdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \cdots & \cdots & \cdots \\ a_{|\mathcal{L}|,1} & a_{|\mathcal{L}|,2} & \cdots & \cdots & a_{|\mathcal{L}|,|\mathcal{S}|} \end{pmatrix} . \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ \vdots \\ z_{|\mathcal{S}|} \end{pmatrix} \leq \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ \vdots \\ b_{|\mathcal{L}|} \end{pmatrix}$$

$$(z_1, z_2, \ldots, z_{|\mathcal{S}|})^T \geq (0, 0, \ldots, 0)^T \text{ and integers.}$$

$\mathbf{Z} = (z_1, z_2, \ldots, z_{|\mathcal{S}|})$ represents the vector of integer variables associated with p-cycles $s \in \mathcal{S}$. Each variable $z_s (s \in S)$ is equal to the number of copies of the p-cycle it is associated with. $\mathbf{C} = (c_1, c_2, , \ldots, c_{|\mathcal{S}}|)$ is the cost vector of all p-cycles. $\mathbf{B} = (b_1. b_2, \ldots . b_{|\mathcal{L}|})$ is a vector of coefficients representing the protection capacity budget on each link $\ell \in \mathcal{L}$. $\mathbf{A} = (a_{\ell,s})$ is a matrix of coefficients, each in $\mathbb{Z}^+$ and equal to the number of protection paths a cycle s can provide to a link ℓ. The expression to be minimized is called the objective function (in this case $\mathbf{C}^T\ \mathbf{Z}$). The inequalities $\mathbf{AZ} \leq \mathbf{B}$ are the constraints that delimit a solution space over which the objective function is to be optimized.

Except for the integrality constraints and the solution methods, Linear Programming (LP) is an optimization model similar to ILP. In LP, the integrality constraints on the optimization variables are dropped. Though, the general form of an LP:

$$\text{Minimize} \quad \sum_{s\in\mathcal{S}} c_s\, z_s$$

subject to:

$$\sum_{s\in S} a_{\ell,s}\, z_s \le b_\ell \qquad \ell = 1,\ 2,\ 3, \ldots, |\mathcal{L}|,$$

$$z_s \ge 0 \qquad s = 1,\ 2,\ 3, \ldots, |\mathcal{S}|.$$

The size of the above LP and ILP optimization models depends on the number of candidate protection p-cycles. Each p-cycle $s \in \mathcal{S}$ is assigned a variable z_s in the objective, and a column $\mathbf{A}^s$ in the constraints. The size of the mathematical model and the integrality constraints on the variables affect the scalability and performance of the solution methods during the optimization process.

4.2.2 ILP Solution Method

Figure 4.1 illustrates the relation between an optimal solution of an ILP and that of its relaxed LP. Therein, we have two p-cycles (two dimensional solution space) and three arbitrary constraints, and the objective is to maximize a linear function Z. The two dashed lines labeled Z^*_{LP} and Z^*_{ILP} give the intersection of the optimization function with the convex hull of the LP and ILP spaces, respectively. The intersection points identify the linear and integer optimal solutions of the LP and ILP problems, respectively. Note that, for this case, rounding down the LP optimal solution gives the ILP optimal solution. However, this is usually not true in practice.

Since LP is less constrained than ILP. the following is deduced:

- If the objective of ILP is a maximization, the optimal objective value for LP is greater than or equal to that of ILP, see Figure 4.1 for an illustration.
- If LP is infeasible, then so is ILP.
- If the optimal LP solution is integer, then the same solution is also feasible and optimal for ILP.

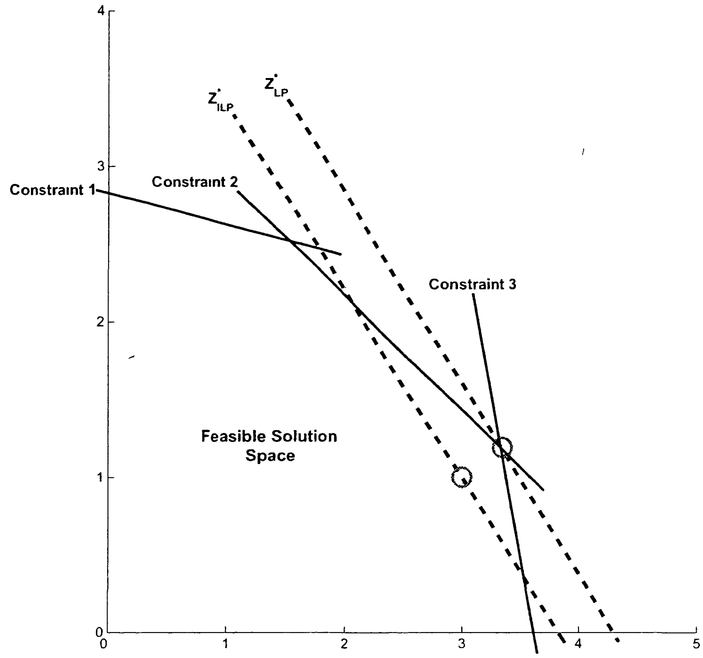


Figure 4.1: LP vs ILP

Even if the mathematical models of LP and ILP look similar, the algorithms used to carry the optimization on those models are completely different. The Simplex algorithm of George Dantzig [Dan98] is the widely used LP solution method in many optimization softwares. Given a polyhedron representing the solution space and a real-valued linear function representing the objective function defined on this polyhedron. the simplex method will find a vertex on the polyhedron, if it exists, where this function has the largest (or smallest) value [BJS08]. The vertices of the polyhedron form the basic feasible solution space of the LP model. In order to solve the LP model, the simplex method starts by constructing an initial feasible solution at a vertex of the polyhedron and explores the solution space by moving along a path on the edges of the polyhedron to vertices with equal or higher (at least lower if a minimization objective) values of the objective function until an optimum is reached. If certain precautions against cycling are taken into account, the simplex algorithm is quite efficient and is guaranteed to find the global optimum of the LP optimization problem (see chapter 3 in [Chv83]).

In contrast to LP problems,.which can be solved efficiently within a limited number of iterations, ILP problems are NP-hard [NW99]. Some solution methods of ILP use their LP relaxations to approach their integer solutions. In fact, solving LP does give a bound on the optimal value of the ILP, and may give the optimal solution to ILP if the LP solution if integer. The ILP formulation plays a major role in the efficiency and scalability of the applied solution method. Indeed, in order to be efficient, ILP solution methods based on LP relaxations require formulation whose LP relaxation gives a good approximation to the convex hull of the integer feasible solutions. Different methods have been proposed to close the gap between LP and ILP, and to boost the performance of the ILP methods [Sch98, Wol00]. In the next section, we review some ILP based solution methods.

Branch and Bound Techniques

Branch and Bound (B&B) [LW66] is a well known optimization technique for its application to ILP problems. This approach computes upper and lower bounds on the optimal objective value during the optimization process; and terminates with an integer optimal solution, or with a certificate proving that the suboptimal point found is ε-optimal (integrality gap) [LW66]. B&B algorithms are basically based on a *divide and conquer* technique. The dividing (branching) is performed by dividing the feasible solution space into smaller subsets. The conquering (bounding) is performed by discarding the current subset if its bound indicates that it cannot contain an optimal solution for the original problem. This technique is widely used in optimization of protection schemes in the literature.

The efficiency of the B&B technique depends critically on the used branching and bounding strategies [LW66, NW88]. Some branching choices could lead to a repeated branching, without any pruning of the B&B tree. In such a case, the branching method would become an exhaustive enumeration of the solution domain, which is very often huge.

Cutting Plane Techniques

An alternate solution to B&B. called cutting planes. can also be used to solve ILP problems [KJ60. JRT95]. The fundamental idea behind cutting planes is to ultimately find the constraints (facets) of the convex hull. In practice, one has to be satisfied with cuts that are not necessarily facets.

Cuts are added to the relaxed LP model until its optimal feasible solution becomes integer. As any feasible integer solution for an ILP problem is also feasible for its relaxed LP problem, and a fractional feasible solution to the LP is not feasible for its constrained ILP, the cutting planes are added to close the gap between LP and ILP by eliminating fractional feasible solutions to the LP model. Finding such cutting planes corresponds to the separation problem of the solution space. This process is repeated until an optimal integer solution is found.

Branch and Cut Techniques

A branch and cut technique is a hybrid of a B&B and a cutting plane technique [CF97, JT98]. In this method, if the obtained solution to the relaxed LP model has fractional values for some integer variables, then a cutting plane algorithm is used to find useful cuts, which are violated by the current fractional solution, but satisfied by all feasible integer solutions. If such cuts are found, they are added to the linear program, and the solution process is repeated until either an integer solution is found or until no more cutting planes are found. In this latter case, the B&B is started to split the solution space by branching on fractional variables.

4.3 Column Generation

Column Generation (CG) is an efficient algorithmic technique for solving large *linear programing problems* but its strength unfolds in solving integer programming problems too. It has lately been widely used in solving some large scale problems such as transportation and scheduling, e.g., air-line, vehicle, crew scheduling [DS89, RS94, CP99a, CP99b], but not yet as much in telecommunications [JRBG07, JRBG07, SPR+07]. Its motivation is that many linear models are too huge to explicitly consider all their variables and constraints, and that in the final optimal solution most of the variables will be non-basic (equal to zero) and only a small subset of them will be basic (take a non negative value). For example, in p-cycle protection based ILP models, there can be thousands to millions of p-cycles, and only a limited number, e.g., 1% or less, will be considered in the optimal protection scheme.

Though, in classical LP and ILP techniques, much effort is spent in exploring a large solution space in order to locate an optimal solution which is a combination of a very small set, e.g., a set of p-cycles in a network.

The idea behind CG is to consider only the variables which have the potential to improve the objective function, by generating them on demand by means of a CG technique identical to generating cutting planes on the corresponding dual problem [Chv83, Las70].

4.3.1 CG Modeling

In CG, the mathematical modeling is not straightforward. Indeed, the modeling process requires some abilities to look at a problem with a different view in order to identify a decomposition structure. The problem being solved by CG techniques is split into two sub problems: a master problem and a pricing problem. The restricted master problem is a linear program with only a subset of variables being considered. The pricing problem is a new ILP model derived from the master problem to identify new promising basic variables for the master problem. The main motivation behind the CG decomposition technique is to delegate the subroutines to the subproblems at a subordinated level, i.e., pricing problem, and to coordinate the linking at a superior level, i.e., the master problem. However, not all LP optimization problems can be expressed in the CG modeling paradigm. The CG modeling approach requires that the whole problem can be decomposed into sub-routines, and that analytical functions can be established between the subproblems through their variables and parameters. The objective function of the pricing subproblem is defined as the reduced cost of the master problem (see below). In the context of protection schemes, these two routines can be optimization of the protection structures at the master problem, and generation of protection structures at the pricing problem.

Following the simplex method to solve the previous LP program illustrated in Section 4.2.1, at each iteration, we search for a non-basic variable to price out and enter the basis. This means that, in the pricing step, we look for the argument (column) of the following optimization function:

$$\arg\min\{\bar{c}_s = c_s - \bar{\mathbf{u}}^T A^s \ : \ s \in S\}. \tag{4.1}$$

An explicit search of S is impractical as the set S of p-cycles is huge. In CG, we work with a reasonable small subset $S' \subseteq S$ of columns associated with p-cycles in a Restricted Master Problem (RMP). If $\bar{\mathbf{z}}$ and $\bar{\mathbf{u}}$ are the optimal primal and dual solutions of the RMP, then, for a set $\mathscr{A} \neq 0$ of columns $A^s, s \in S$, the following subproblem gives an answer to the pricing problem.

$$\bar{c^*} = \min\{\bar{c}_s = c(A) - \bar{\mathbf{u}}^T A \ : \ A \in \mathscr{A}\}. \tag{4.2}$$

If $\bar{c^*} \geq 0$, then no negative reduced cost $\bar{c}_s$ exists: $\bar{\mathbf{z}}$ is the optimal solution of the current RMP and of the original master problem as well. Otherwise, the column returned by the current pricing problem is added to the RMP.

4.3.2 CG Solution Method

The advantage of solving the optimization problem in (4.2) over the one in (4.1) is related to the size of the pricing solution space $\mathscr{A}$. The set of all p-cycles S cannot be explicitly considered as in (4.1), while in (4.2) it is a subset of p-cycles that are considered. The whole CG optimization process for p-cycle protection is repeated as follows.

Algorithm 1 Column Generation Solution Method

```
Initialize the RMP with a feasible solution, e.g., a set of p-cycles providing 100% protection.
repeat
  solve the RMP, we obtain dual prices for each of the constraints in the RMP problem. This
  information is then utilized in the objective function of the pricing problem.
  solve the pricing problem
  if objective value is negative then
    a variable with negative reduced cost associated to a potential cycle has been identified,
    this variable is then added to the master problem.
  else
    the current RMP solution is optimal
  end if
until the current RMP solution is optimal
```

To initiate the CG solution method, an initial feasible solution (set of protection p-cycles) to the RMP is required in order to ensure that proper dual information is passed to the pricing problem. Depending on the application, it is not always obvious to construct an initial feasible solution of the RMP. A common approach is to use a two-phase method similar to the two-phase approach incorporated in the simplex method in order to find an initial basic feasible solution. A solution approach in our p-cycle optimization is to add a set of artificial p-cycles with a large positive cost. This approach guarantees a feasible solution to the LP relaxation problem. Further details on initialization, especially in MILP are given in [LD05]. The initial feasible solution to the LP relaxation is very important in the CG solution process. Poorly chosen initial columns may lead to more iterations when the resulting initial solution is far away from the optimal one.

The overall CG solution process is illustrated in the following flowchart:

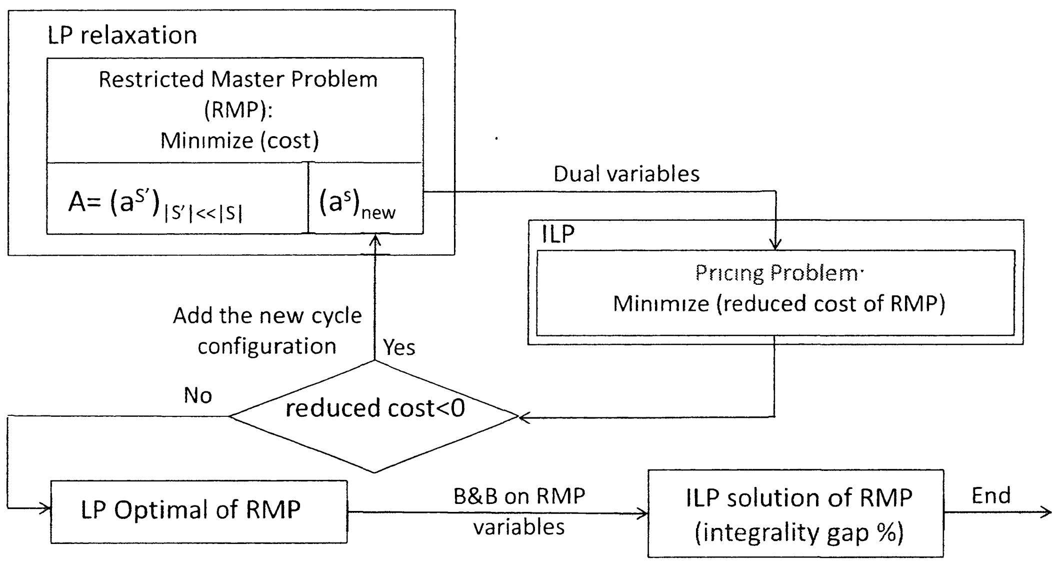


Figure 4.2: CG Solution Process

The RMP is a linear relaxation of the original master ILP. though, it can be solved with any LP solution method. The ILP pricing problem is to find a column with the lowest negative reduced cost (highest positive reduced cost if a maximization problem). However, it is not necessary to select the columns with the lowest reduced cost in order to find the optimal solution of the LP. any column with a negative reduced cost can be enough to be able to iterate Based on that, the pricing efficiency can be improved by stopping its execution once its cost is lower than a given negative threshold or 0 [VBJ+98, DDS05]. Furthermore, in the pricing problem, it may be possible to generate more than one column during an iteration. Such an approach increases the size of the RMP more quickly and may reduce the number of required iterations to reach the optimal solution [LD05, Ogt02]. In the CG solution approach for ILP, we are concerned by mechanisms to find an integer solution for the original master problem, and at the same time, to solve the linear relaxation of the RMP. The LP relaxation of the RMP solved by CG may not be an integer feasible solution, and applying a standard B&B technique to the RMP is also unlikely to find an optimal, or even a feasible integer solution to the original problem. However, the value of the current RMP optimal solution gives an insight on how possibly far (bound) the ILP value is from the optimal value of the RMP. Though, if the RMP has an integer feasible solution which is ε-optimal, then, this solution may be the optimal solution of the original ILP. Considerable efforts have been spent on the topic of how to obtain an integer solution by combining CG approach and other ILP optimization tools. Some branching strategies in CG are presented in [Van06, Van00], and a rich literature on CG and B&B can be found in [BJN+98, VW96, LD05, Van94].

In this thesis, we propose a set of optimization methods of protection schemes based on CG where we solve the LP problem, and branch on the continuous variables of the RMP (as illustrated in flowchart 4.2). We found optimal solutions to the ILP problems with a very low optimality gap (ε) in almost all solved problems ($\varepsilon \in [0\%, 5\%]$). Though, we refrained from adding any branch-and-price or branch-and-cut ILP schemes to our CG solution methods.

CHAPTER 5

p-Cycle Based Protected Working Capacity Envelope

5.1 Introduction

The trends in optical transport networks are moving toward dynamic network models that will support on-demand set up, modification and release, of a wide range of services and the ability for each class of services to be defined and treated separately. Dynamic network models will help service providers to maximize their profitability through automated provisioning of optical services. To address the dynamic and cost-effective network models. there is a need for an efficient network-control model to cope with the operational expenditures (OPEX) associated with the management and deployment of services. Standard-based protocols will help providers in savings, by enabling them to integrate multi-vendor equipment in their networks. These novel trends are under standardization in the automatic switched optical network (ASON) [Rec01] and the generalized multi-protocol label switching (GMPLS) frameworks [M+04, Ber03b].

In survivable optical networks. particularly in WDM networks, dynamic provisioning involves two inter-related capacity planes: The working plane and the protection plane. Design and planning of these two planes require high attention as they should be at the same time, packed tightly and disjoint in order to optimize the deployment cost. Such a requirement increases the complexity of the management process to maintain consistent network states, and efficiently provide resiliency in the network.

The problem of dynamically provisioning protected working capacity has been extensively studied within the paradigm of a working primary path and a predetermined link (or node) disjoint backup path, both established end-to-end at the provisioning time [SZM05, LR06, SSM03, KL03, YADA01]. In order to reduce the bandwidth requirement, shared backup protection schemes, e.g., Shared Backup Path/Segment/Link Protection (SBPP/SBSP/SBLP) [KL00, XXQ02, HM04, SR01, OZZ+04] have been widely used. Under shared protection techniques, backup paths are allowed to share spare capacity, provided that their protected working paths do not belong to the same SRG. These sharing techniques improve the capacity efficiency of the protection design. but they involve complex network operations and a larger state information related to the disjointness among working and protection paths. Indeed, the requirement for an establishment of a shared-capacity protection path is highly dependent on the state information of all ongoing lightpaths in the network (available capacity and sharing conditions of backup capacities), which is not easy to maintain accurately as the network scale or when the velocity of the network traffic increases [KL00]. In order to simplify the provisioning operations and make them as independent as possible of the network state information, Grover has proposed a new design paradigm in survivable WDM networks named the Protected Working Capacity Envelope (PWCE) [Gro04b].

In this Chapter, we focus on PWCE, and propose efficient and scalable methods to design optimized PWCE with different network models including link and network spare capacity budgets. We use simple (elementary) and non-simple p-cycles as protection building blocks. and elaborate further on their ability to efficiently use the spare capacity. The particular contribution in this chapter is related to the scalable and efficient optimization strategies based on CG that can be used within different design conditions, and the new non-simple p-cycle approach that is shown more efficient than the simple p-cycle one.

5.2 The PWCE Paradigm

The PWCE paradigm was first exposed in [Gro04b], and later studied in detail in [She06]. In PWCE, the protection capacity is deployed ahead of any working capacity or network failure in order to protect the network resources, though, potential working capacity. In the PWCE concept, given a demand forecast and a link or a network spare capacity budget, the problem consists to find an optimized protection plane to meet the potential working capacity of the traffic forecast.

Figure 5.1 illustrates the design process in the PWCE paradigm. The optical transport network with its link transport capacity (number of wavelength channels) as illustrated in the top of Figure 5.1, is divided and optimized to provide as much as possible of protected capacity (maximum size PWCE). The illustrated link spare capacity budget on the left of Figure 5.1 enables the protection of the illustrated link capacity budget on the right of the same figure In PWCE. it is the pre-deployed protection capacity that defines the PWCE shape and size.

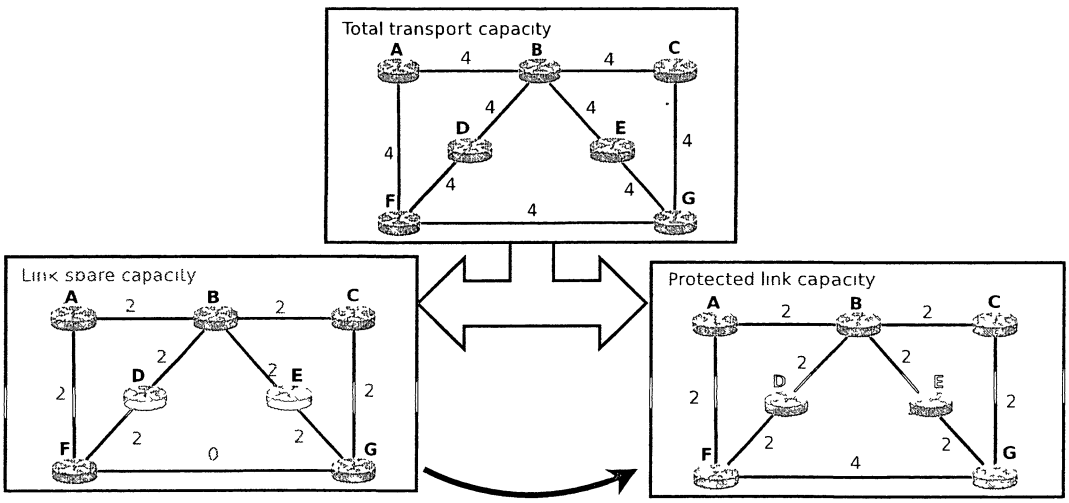


Figure 5.1: PWCE Design Process

Rather than explicitly provisioning protected capacity (working + protection) for each connection, dynamic provisioning algorithms within the PWCE concept perform survivability provisioning over the already protected capacity. After the partitioning of the total transport capacity as illustrated in Figure 5.1. any working capacity can be routed through the envelope provided that the used links have some implicitly protected capacity left. Though, dynamic provisioning of protected capacity is restricted only to the provisioning of working capacity. Further details about state advertisement, network management overhead, and adaptive PWCE can be found in [SG05, She06].

5.3 Design of PWCE

The spare capacity used to set up protection paths can be either configured on the fly to respond to any protection need, or can be end-to-end pre-configured and used in case of a failure. In the design of PWCEs, as in classical protection schemes, the protection capacity can be either reserved and configured dynamically in case of a failure, or fully pre-cross connected ahead of failures.

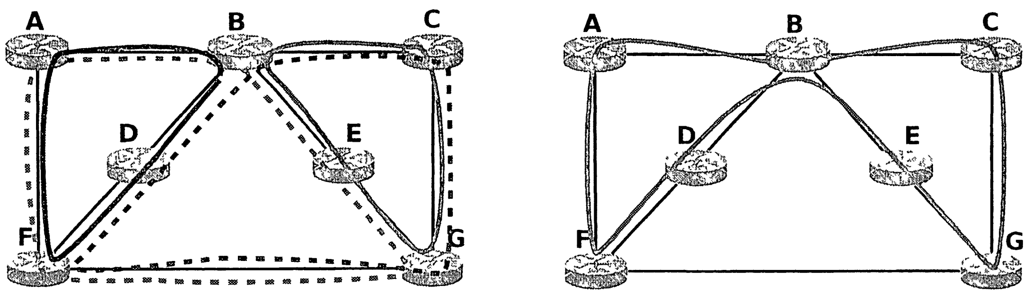
In order to minimize the recovery delay and simplify the provisioning operations in the PWCE paradigm, we adopt the fully pre-cross connected p-cycle protection approach. By using p-cycles in the design of PWCEs, we aim at gathering the advantages of the PWCE design approach and the p-cycle protection method. Indeed, the p-cycle based PWCE approach allows pre-deployment of fully pre-cross connected structures, which enable fast recovery of traffic with a limited reconfiguration in the underlying protection plane.

5.3.1 p-Cycle Based PWCE

The design problem of p-cycle based PWCE can be defined as a combinatorial problem consisting to find an appropriate set of p-cycles to protect the maximum capacity in the network for a given link/network spare capacity budget that is known in advance.

Figure 5.2 illustrates two optimal designs of survivable WDM networks based on PWCE using p-cycles. The transport capacity budget of the network is illustrated in Figure 5.1: All links are assigned a transport capacity equal to four channels of the same capacity. Two types of p-cycles are used in these two protection schemes in order to maximize the size of the designed PWCE: The simple and non-simple p-cycles. The simple p-cycle based scheme includes all elementary p-cycles, i.e., p-cycles that pass through each node in the network at most once. The non-simple p-cycle based scheme includes all possible p-cycles in the network[1], i.e., there is no limit on the number of times a p-cycle can pass through any node. This means that the simple p-cycle set is a subset of the non-simple one.

In Figure 5.2-(a), the illustrated protection scheme contains four simple p-cycles. Figure 5.2-(b) contains two copies of the illustrated single non simple p-cycle. The objective function of these two designs is to maximize the PWCE size with a link spare capacity budget $\leq 50\%$ on each link, i.e., 2 channels.



(a) Simple p-cycle

(b) Non-Simple p-cycle

Figure 5 2: Simple and Non-Simple p-Cycle Based PWCEs

	simple p-cycle		non-simple p-cycle	
Links	w_ℓ^P	w_ℓ^W	w_ℓ^P	w_ℓ^W
{A.B}	2	2	2	2
{A,C}	2	2	2	2
{A,D}	2	2	2	2
{A,E}	2	2	2	2
{C,G}	2	2	2	2
{B,F}	2	2	2	2
{E.G}	2	2	2	2
{D,F}	2	2	2	2
{F,G}	**2**	**2**	**0**	**4**
Total	**18**	**18**	**16**	**20**

Table 5 1: Capacity Distribution in Simple and Non-Simple p-Cycle Based PWCEs

Table 5.1 illustrates the optimized partitioning of the total transport capacity over the protection and working planes. The w_ℓ^P and w_ℓ^W values represent the link protection budget and the resulting

[1]Excluding p-cycles that may pass through a link more than once

protected capacity on each link ℓ, respectively. We see in Table 5.1 that the non-simple scheme uses more efficiently the spare capacity to provide a larger size PWCE than the simple p-cycle scheme. The non-simple cycle in Figure 5.2-(b) uses less spare capacity (16 channels) and provides larger protected capacity (20 channels) than the simple p-cycle based scheme in Figure 5.2-(a), which uses 18 spare channels and provides only 18 protected channels (100% redundancy). Obviously, as the set of simple p-cycles is a subset of the set of non-simple p-cycles, the size of the PWCE provided by the non-simple p-cycles is at least as large as that provided by the set of simple p-cycles.

5.3.2 Prior Work on Design of PWCE

Conventional design methods of PWCE based on p-cycles have tackled the problem by a two-step approach [SG04b, SG05, ZZB05, SG03a, RT05]. The first step deals with the enumeration of all/(set of) p-cycles in the network to form a potential candidate set; and the second step selects the most promising subset of p-cycles from the candidate set using ILP (Integer Linear Program) optimization methods [SG03a, Sch02]. However, as explained in Chapter 4, the size of the candidate p-cycle set grows exponentially as the network size increases, and from this results large ILP models, which in turn, makes the classical ILP optimization algorithms very time-consuming and not scalable.

To address the scalability issue, different polynomial time algorithms for selecting a limited number of p-cycles have been proposed in the literature [DHGY03, ZY02a]. These algorithms are elaborated to select a subset of valuable p-cycles (based on some metrics, see Sections 3.1.4 and 4.1.2 for examples of metrics) that contains the potential candidates for the ILP optimization step. Obviously, the selected p-cycles are individually efficient, but when combined together, they generally provide only a suboptimal solution which is not necessarily close to the optimal one (see Section 5.5). However, those algorithms allow an interesting trade off between the scalability of the optimization method and the quality of the solutions. Furthermore, the adopted design metrics have been very often based on a single protection parameter, e.g., protected capacity or protection capacity. which does not reflect the real dimension of the PWCE design problem. Indeed. not all links have the same link spare capacity budget and same potential working capacity in the network, though, most of the candidate p-cycles will be either impossible to set up because of a limited spare capacity budget, or will be providing more or less protected capacity that what is needed.

In the design of survivable WDM network based on PWCE, only simple p-cycle building blocks have been considered. The advantages of using non-simple p-cycles over simple p-cycles in WDM networks were discussed in [Gru03]. Therein, different types of non-simple p-cycles were illustrated, and an ILP optimization model was proposed. The proposed ILP optimization method was a two-step based approach where a subset of non-simple p-cycles (only p-cycles of a limited length) were enumerated ahead of an optimization method which consisted to maximize the grade of service. The set of non-simple p-cycles is larger than the simple p-cycle set, though, this design approach is impractical and can never scale even in medium size networks. Furthermore, because the considered potential p-cycles are only a subset of the global set of non-simple p-cycles, the resulting solution is not necessarily a global optimal solution, rather, it is a local optimal solution.

5.3.3 Discussion and Further Considerations

As pointed out in previous Sections 4.1.2 and 3.1.4, the prevalent design approach consisting to pre-enumerate (all or a selection of) candidate p-cycles before the optimization approach is not practical nor scalable. The main drawback of this design approach lies in the enumeration step of the candidate p-cycles. In the selection process, the properties of the p-cycles are usually considered independently of the network conditions, e.g., link spare capacity budget and traffic distribution. This inevitably leads to excessive enumeration of inappropriate p-cycles.

In the next section, we propose a new design approach of PWCE using the large scale CG optimization tools. In contrast with the two-step conventional design approach, a CG based method does not require an a priori explicit enumeration of all/(a set of) p-cycles in the network. A limited number of relevant p-cycles are dynamically generated during the optimization process only when they are needed in order to improve the current LP solution. Though, it results in a compact model with a small number of variables, which is solvable by the highly scalable CG approach.

5.4 Efficient and Scalable Design of p-Cycle Based PWCE

In this section, we propose a CG-based method where the p-cycle enumeration and the optimization processes are jointly performed dynamically by two complementary problems. Both the link spare capacity budget and the potential working capacity are integrated as design parameters and considered in the generation process of potential p-cycles. Recall that a CG formulation relies on a decomposition of the initial problem into the so-called *master* and *pricing* problems, see, Chapter 4 for a basic background). In our CG optimization approach of p-cycle based PWCE, the RMP (operates on a restricted set of p-cycles generated dynamically by the pricing problem) maximizes the PWCE size according to a set of capacity (working and protection) constraints. At each iteration, the RMP is solved and provides the values of the dual variables which are necessary for solving the pricing problem. The output (solution) of the pricing problem is a new promising p-cycle which is added to the RMP. The augmented master and pricing problems are solved alternatively until no more promising p-cycles can be found, i e., no more p-cycles with a positive (assuming the master problem is a maximization problem) reduced cost can be found.

The design problem of a p-cycle based PWCE can be described as follows: Given a link or network spare capacity budget and a network traffic forecast, find the optimal combination of p-cycles that will maximize the protected capacity (or at least protect the forecasted traffic demands). In the next subsection, we present our CG based formulation for the design of optimized p-cycle based PWCE.

5.4.1 Master Problem

The master problem takes care of the capacity constraints, i.e., the working capacity and of the spare capacity of the potential p-cycles. For both simple and non-simple p-cycles, we develop the same master problem as in both optimization problems we deal with the selection of p-cycles. We denote the number of protected working capacity units on a link ℓ in the network by w_ℓ, which is less or equal to the maximum (total) transport capacity (w_ℓ^F) of link ℓ: $w_\ell \leq w_\ell^F$ for all $\ell \in \mathcal{L}$. We suppose that we are given a link spare capacity budget Ψ^F ($\psi_\ell^F \leq \alpha_\ell . w_\ell^F . \alpha_\ell$ a real $\in \{0, 1\}$) which will be used for the setup of protection capacity w_ℓ^P.

Our objective is to maximize the number of working link-channels w_ℓ according to a certain distribution $U(u_\ell)$ in the network, so the objective function is:

$$\max \sum_{\ell \in \mathcal{L}} u_\ell w_\ell.$$

As in [GS00], we use bidirectional p-cycles, therefore, straddling-cycle links can be protected in two ways, as two restoration paths are available for each unit of p-cycle. We define two parameters a_ℓ^s and b_ℓ^s in order to configure the p-cycles: a_ℓ^s gives the number of protected channels on link ℓ by the p-cycle s, and $b_\ell^s \in \{0, 1\}$ counts the used capacity by p-cycle s along each link ℓ:

$$a_\ell^s = \begin{cases} 2 & \text{if } \ell \text{ is a straddling-cycle link in } p\text{-cycle } s \\ 1 & \text{if } \ell \text{ is an on-cycle link in } p\text{-cycle } s \\ 0 & \text{otherwise.} \end{cases}$$

$$b_\ell^s = \begin{cases} 1 & \text{if } \ell \text{ is an on-cycle link in } p\text{-cycle } s \\ 0 & \text{otherwise.} \end{cases}$$

The variables of the optimization problem are w_ℓ and $z^s \in \mathbb{Z}^+$, which are the number of protected working capacity units on link ℓ and the thickness (number of copies) of unit-capacity p-cycle s, respectively.

The constraints of the master problem are:

$$\sum_{s \in S} a_\ell^s z^s - w_\ell \geq 0 \qquad \ell \in \mathcal{L} \tag{5.1}$$

$$\sum_{s \in S} b_\ell^s z^s + w_\ell \leq w_\ell^F \qquad \ell \in \mathcal{L} \tag{5.2}$$

$$\sum_{s \in S} b_\ell^s z^s \leq \psi_\ell^F \qquad \ell \in \mathcal{L} \tag{5.3}$$

$$w_\ell \geq w_\ell^{\min} \qquad \ell \in \mathcal{L} \tag{5.4}$$

$$w_\ell, z^s \in \mathbb{Z}^+ \qquad \ell \in \mathcal{L}, s \in \mathcal{S}. \tag{5.5}$$

Constraints (5.1) guarantee a link protection for w_ℓ working channels along each link ℓ. Constraints (5.2) prevent the overall working and protection capacity of link ℓ from exceeding its transport capacity (w_ℓ^F). Constraints (5.3) impose a link spare capacity budget. Constraints (5.4) impose a minimum protected working capacity ($w_\ell^{\min}$) along each link. Constraints (5.5) are integrality constraints. Observe that the master problem is expressed in terms of variables indexed dynamically by $s \in S$. The dynamic set S grows as long as the pricing problem is able to generate columns (cycles) with a positive reduced cost, i.e., promising p-cycles that can improve the value of the objective function of the LP relaxation of the master problem.

5.4.2 Simple p-Cycle Pricing Problem

The pricing problem corresponds to the optimization problem of maximizing the reduced cost associated to variables z^s in the master problem. The simple p-cycle pricing problem generates simple p-cycles to protect working capacity in the network. We define the variables of the pricing problem as follows:

$$x_\ell^o = \begin{cases} 1 & \text{if } \ell \text{ is an on-cycle link in the current } p\text{-cycle} \\ 0 & \text{otherwise,} \end{cases}$$

$$x_s^s = \begin{cases} 1 & \text{if } \ell \text{ is a straddling-cycle link in the current } p\text{-cycle} \\ 0 & \text{otherwise,} \end{cases}$$

We also need the following sets:

For all $v \in \mathcal{V}$, the set of adjacent links to node v

$$\mathcal{E}(v) = \left\{ \ell_j : \ell_j = \{v, v_i\} \in \mathcal{L} \right\},$$

For all $\ell \in \mathcal{L}$, the set of two end-nodes of link ℓ:

$$\mathcal{V}(\ell) = \left\{ v_i, v_j : \ell = \{v_i . v_j\} \right\},$$

and, for all $N \subseteq \mathcal{V}$, the cocycle of N, i.e., the set of links such that one of its end-node belongs to N and the other does not:

$$\mathcal{E}(N) = \left\{ \ell : \ell = \{v_i, v_j\} : v_i \in N, v_j \in \mathcal{V} \backslash N \right\}.$$

The objective function of the pricing problem, i.e., the maximization of the reduced cost can be written as follows,

$$\max \left(\sum_{\ell \in \mathcal{L}} a_\ell^s \theta_\ell^1 - \sum_{\ell \in \mathcal{L}} b_\ell^s \theta_\ell^2 - \sum_{\ell \in \mathcal{L}} b_\ell^s \theta_\ell^3 \right),$$

where θ_ℓ^1, θ_ℓ^2, θ_ℓ^3 are the dual variable vectors associated with constraints (5.1), (5.2) and (5.3), respectively. These dual variables contain an important information about the protected capacity, the used capacity, and the available spare capacity after each iteration. When expressed in terms of the variables of the pricing problem, the objective function becomes equivalent to.

$$\max \left(\sum_{\ell \in \mathcal{L}} \left(\theta_\ell^1 - \theta_\ell^2 - \theta_\ell^3\right) x_\ell^o + 2 \sum_{\ell \in \mathcal{L}} \theta_\ell^1 x_\ell^s \right).$$

The constraints of the pricing problem are defined in order to shape the generated p-cycles. They can be written as follows:

$$\sum_{\ell \in \mathcal{E}(v)} x_\ell^o \leq 2 \qquad v \in V \tag{5.6}$$

$$\sum_{\ell' \in \mathcal{E}(v)\ \ell' \neq \ell} x_{\ell'}^o \geq x_\ell^o \qquad v \in V, \ell \in \mathcal{E}(v) \tag{5.7}$$

$$4 x_\ell^s \leq \sum_{v \in \mathcal{V}(\ell)} \sum_{\ell' \in \mathcal{E}(v)} x_{\ell'}^o \qquad \ell \in \mathcal{L} \tag{5.8}$$

$$\sum_{\ell \in \mathcal{E}(N)} x_\ell^o \geq x_{\ell'}^s \qquad N \subset V, \ell' \in \mathcal{E}(N) \tag{5.9}$$

$$x_\ell^o . x_\ell^s \in \{0.1\} \qquad \ell \in \mathcal{L}. \tag{5 10}$$

All nodes belonging to a given cycle are required to have at most two incident links in the cycle. This is ensured by the sets of constraints (5.6) and (5.7). Constraints (5 6) set the upper bound on the number on incident links, and constraints (5.7) set that bound to either two or zero. Constraints (5.8) guarantee that if a link straddles the current p-cycle, then each of its end-nodes is also adjacent to two links that are on-cycle ones. Constraints (5.9) guarantee that if a link is straddling a p-cycle, then both of its end-nodes belong to the same cycle. Constraints (5.8) and (5.9) together guarantee that if a link ℓ is straddling a cycle, then any network cut separating its two end-nodes should contain two on-cycle links. The size of the set of constraints (5.9) is equal to the number of cuts separating all node pairs in the networks. Their enumeration would be impossible or results in a huge ILP model. In this case, and in order to scale the pricing model in large networks, we only add a few of them at the beginning of the optimization process, and others only when they are violated. Indeed, most of these cuts will not be useful and will not be binding in the optimal solution. Let

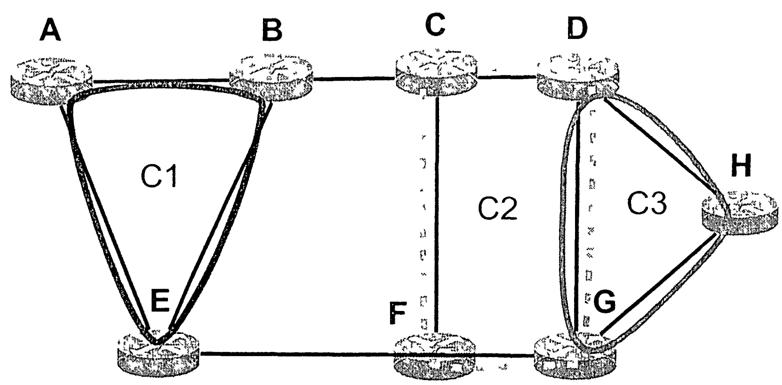


Figure 5.3: Generated p-Cycles by the Pricing Model

us look at an example in Figure 5.3 to illustrate the purpose of these last two types of constraints. The pricing problem can generate any of the p-cycles C_1, C_2 or C_3 on an individual basis, but it can also generate the p-cycles C_1 and C_3 simultaneously. However, note that p-cycles C_2 and C_3 cannot be generated simultaneously because of constraints (5.8) and (5.9) which do not allow a link to straddle two different p-cycles.

Though, each iteration of the pricing problem can generate more than one elementary p-cycle, and can avoid counting protection working capacity straddling different p-cycles. This is helpful in minimizing of the number of calls to the pricing problem.

5.4.3 Non-Simple p-Cycles Pricing Problem

The only difference between the non-simple p-cycle pricing problem and the simple one is in the shape of the protection structures. In the non-simple p-cycle scheme, a p-cycle can pass through a node more than once. Though, it can protect more straddling-cycle links (see Figure 5.2 for an example). The reduced cost of the master problem does not change, hence the pricing optimization objective of the non-simple p-cycle remains the same.

The constraints of the pricing problem are updated as follows: Constraints (5.6) and (5.7) are replaced by constraints (5.11). Constraints (5.8) to (5.10) are kept as in the previous simple p-cycle model, and we add constraints (5.12).

$$\sum_{s \in \mathcal{E}(v)} x_\ell^o = 2n_v \qquad v \in V \qquad (5.11)$$

$$x_\ell^s + x_\ell^o \leq 1 \qquad \ell \in \mathcal{L} \qquad (5.12)$$

$$n_v \in \mathbb{Z}^+ \qquad v \in \mathcal{V} \qquad (5.13)$$

All nodes spanned by a p-cycle are required to have an even number of incident links in the p-cycle, which is ensured by constraints (5.11). Constraints (5.12) say that a link ℓ cannot be a straddling-cycle and an on-cycle link at the same time. In this non-simple p-cycle model, two end-nodes of an on-cycle link can have more than two incident links in the underlying p-cycle. Though, to avoid any confusion with a straddling-cycle link, we used the set (5.12) of constraints. Constraints (5.13) are additional integrality constraints.

5.5 Numerical Results

In this section, we evaluate the performances of the two protection methods base on simple and non-simple p-cycles, respectively.

5.5.1 p-Cycle Protection Model

In addition to our CG-based approach, we consider two other approaches for enumerating p-cycles. The first approach [SG03a, SG04b, Sch02, GS00] is based on an exhaustive enumeration of all p-cycles in the network. The second one [ZY02a, DHGY03] is based on a selective enumeration of a restricted set of valued p-cycles. We consider three methods of selective enumeration, which have appeared in the literature: The *Straddling Link Algorithm (*SLA*)* [ZY02a], and the GROW and EXPAND ones of [DHGY03]. These methods are used as p-cycle suppliers to an ILP formulation (our master problem). The first method (denoted by B-ILP) is a brute force approach based on an exhaustive enumeration. The three other methods are S-ILP for ILP based on SLA procedure of [ZY02a], E-ILP and G-ILP for ILP based EXPAND and GROW procedures of [DHGY03], respectively. Note that the resulting ILP models differ from the column generation model in the way the p-cycles are generated (off-line vs. on-line), and also in their number of candidate p-cycles (large to huge vs. very limited).

5.5.2 Network Instances

Table 5.2 presents the network instances used in the comparison of the solution methods considered in this study. The characteristics of each physical topology are as follows: For each network, we provide the number of nodes and links, the average network degree and the standard deviation of the node degrees (which measures the spread of the values of node degrees).

Networks	# Nodes	# links	Avg. Degree	σ(Degree)
NSF [SG03a]	14	21	3.81	0.83
COST239 [SG03a]	11	26	4.72	0.61
USA [MK97]	28	45	3.21	0.97
France [DHGY03]	43	71	3.23	1.41
BRASIL [NR06]	27	68	5.11	1.5

Table 5.2: Network Instances

5.5.3 Simple p-Cycle Based PWCE

In this section, we compare the performance of the CG optimization method of p-cycle based PWCE with the ILP optimization one based on the four different enumeration strategies evoked above.

Comparison metrics

We compare the quality of the solutions obtained by the considered models based on the classical evaluation metrics (redundancy, runtime, capacity efficiency) and the following two new design metrics:

$$\text{Protection gap ratio} = \frac{\sum\limits_{\ell \in \mathcal{L}} \text{unprotected capacity on } \ell}{\sum\limits_{\ell \in \mathcal{L}} \text{protected capacity on } \ell}$$

which gives the ratio of unprotected working capacity over the protected one in the network, and

$$\text{Protection overhead ratio} = \frac{\sum\limits_{\ell \in \mathcal{L}} \text{protection overhead on } \ell}{\sum\limits_{\ell \in \mathcal{L}} \text{protection capacity on } \ell}$$

where the protection overhead is defined as the difference between the amount of potential protected capacity that can be provided by the current protection plane and the effective working capacity that is protected. The protection overhead ratio gives the fraction of spare capacity, which is not protecting any working capacity along some links.

Numerical results in the example below show that, very often, those two ratios are not equal to 0. The explanation is that *(i)* the design and the deployment of p-cycles are performed independently of the available capacity, and *(ii)* the transport capacity on each link varies from one link to the next (alternating links with high and low capacities).

Protection Gap and Protection Overhead: An Example

Let us consider the p-cycle scheme example shown in Figure 5.4, where the labels on the links correspond to their transport capacities (w_s^F). Assume that. in a first step, the protection plane is made of p-cycles C_1 and C_2. each of them with one unit spare capacity (wavelength channel).

The illustrated p-cycle protection scheme shows a protection overhead, and does not guarantee 100% protection to all non-protection capacity (protection gap). In Figure 5.4, p-cycles C_1 and C_2

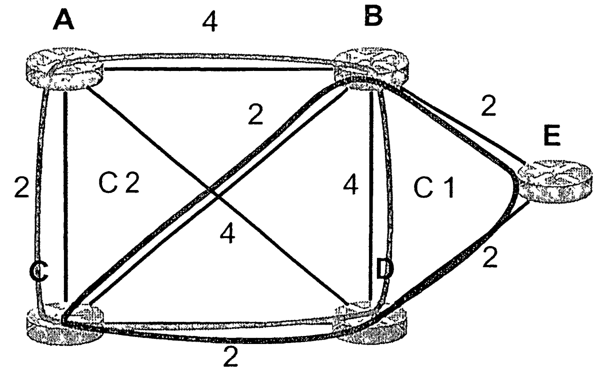


Figure 5.4: Protection Gap and Protection Overhead

are configured with one light channel along all their on-cycle links. Therefore, they can provide one protected working channel for each on-cycle link and two for each straddling-cycle link. Let us first have a look at the protection gap. Links $\{A, B\}$ and $\{A, D\}$ have, each, a total protection gap of two link-channels. Indeed, link $\{A, B\}$ has a total of four transport channels, one channel is used as a spare capacity channel by p-cycle C_2, which provides one protected working channel, and the remaining two link-channels are not protected by the current protection plane, thus, it results in a protection gap of 2 link-channels. Link $\{A, D\}$ is a straddling-cycle link in p-cycle C_2 and can have up to two protected working channels by C_2. This leaves two channels that cannot be protected, hence a protection gap of 2 channels along $\{A, D\}$.

Regarding the protection capacity overhead, the proposed protection plan has a protection overhead of four channels along links $\{B, C\}$ and $\{C. D\}$. Indeed, $\{B. C\}$ is an on-cycle link in p-cycle C_1 and a straddling-cycle link in p-cycle C_2, it is supposed to have up to $2 + 1$ protected working channels, but only one is available, therefore it results in a capacity overhead of $3 - 1$ channels. Link $\{C, D\}$ is an on-cycle link in p-cycles C_1 and C_2, it is supposed to have up to $1 + 1$ protected working channels, but as all the available transport capacity along this link is consumed as protection capacity by p-cycles C_1 and C_2, there cannot be any channel along this link that can be associated with a protected working capacity unit. leading therefore to a protection overhead of two channels.

The link capacity distribution of the proposed protection plane is summarized in Table 5.3, where $w_\ell^{\max}$ is the maximum transport capacity (number of transport channels), w_ℓ^W is the protected working capacity and w_ℓ^P is the used protection capacity.

link	w_ℓ^{max}	w_ℓ^W	w_ℓ^P
{A,B}	4	1	1
{A,C}	2	1	1
{A,D}	4	2	0
{C,D}	2	0	2
{D,E}	2	1	1
{E,B}	2	1	1
{B,D}	4	3	1
{B,C}	2	1	1

Table 5.3: Capacity Distribution

From Table 5 3, we have 10 protected working channels and 8 protection channels (by summing along the w_ℓ^W and w_ℓ^P columns respectively). The protection gap can be calculated as:

$$\sum_{\ell \in \mathcal{L}} (w_\ell^{max} - w_\ell^W - w_\ell^P);$$

it is equal to $22 - 10 - 8 = 4$ (as detailed above)

The protection overhead is equal to:

$$\sum_{s \in S} (2n^{\text{STRA}} + n^{\text{ON-CY}}) z^s - \sum_{\ell \in \mathcal{L}} w_\ell^W$$

where n^{STRA}, $n^{\text{ON-CY}}$ are the number of straddling and on-cycle links, respectively. z^s is the number of copies of p-cycle s. Therefore, the proposed protection plane has a protection overhead equal to $(2 \times 1 + 4) \times 1 + (2 \times 2 + 4) \times 1 - 10 = 14 - 10 = 4$ channels.

We deduce:

$$\text{Protection gap ratio } = 4/10 = 40\%.$$

$$\text{Protection overhead ratio } = (14 - 10)/8 = 4/8 = 50\%.$$

The optimal solution to this PWCE design problem obtained by the CG-based solution method proposed in Section 5.4.2, is given in Figure 5.5. Both the associated protection gap ratio and the protection overhead ratio are equal to zero in this optimal design.

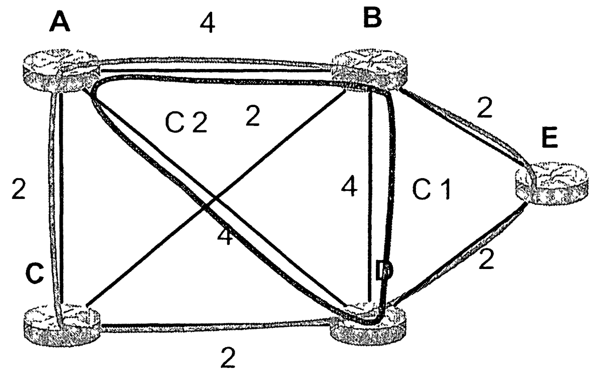


Figure 5.5: Optimal Design of PWCE

Recall that not all the optimal solutions have a protection gap and overhead equal to zero, but it is of interest to keep these two design parameters as small as possible in order to increase the efficiency of the PCWE design methods (illustrative examples are shown in Section 5.5.4).

The protection gap and the protection overhead can be linked to the forcer concept studied in [GM00] (forcer-link is a link such that any increase in its protected working capacity implies an increase in the total spare capacity budget of the network). A link with a nonzero protection gap is a forcer-link. although it has an available working (but unprotected) capacity. A link with protection overhead is a forcer link, because no additional working capacity is possible along the link with the current protection plan.

5.5.4 Simple p-Cycle Numerical Results

Two design qualities are sought in this work, scalability and efficiency. The scalability is evaluated through the number of generated p-cycles and the runtime of the optimization methods. The efficiency is evaluated through the capacity redundancy. the protection gap and overhead ratios.

Our comparison experiments are classified into two classes: In the first class. we consider that all the fibers have the same transport capacity (80 channels/fiber), and in the second class (Table

5.9), we adopt a random transport capacity distribution on fibers and investigate the impact on the efficiency of the proposed and studied design methods.

Based on the size and connectivity of the network instances, we classified the experiments into two categories. Tables 5.4 to 5.6 present the results of the tests performed on the first category of network instances (NSF, COST239, and USA), i.e., networks of relatively small size. In the right most column, we provide the optimal solution (maximum PWCE) using the CG-based approach. The other columns, with headers B-ILP, S-ILP, E-ILP, G-ILP, contain the values of the ILP models derived from a set of p-cycles enumerated by: DFS explicit enumeration of all p-cycles, SLA [ZY02a], EXPAND, and GROW [DHGY03], respectively.

Tables 5.4 to 5.6 show the results obtained on the first three network instances. The observations are the same for all three network instances: The set of p-cycles generated by the S-ILP, E-ILP, G-ILP and B-ILP models is getting larger with each model as the network size increases (the increase is in the order of the number of links). This translates of course in increasing computing times. The B-ILP solution method is, by far, the most time consuming among the compared methods. Indeed, the computing time required for the p-cycle enumeration and the optimization of the resulting huge ILP model for B-ILP is 300, 3800 and 6300 times more than that of S-ILP, E-ILP and G-ILP respectively for the USA network.

	NSF				
	S-ILP	E-ILP	G-ILP	B-ILP	CG
# of potential p-cycles	18	31	88	138	3
Computing time (sec.)	0.02	0.03	0.04	0.7	0.03
# of selected p-cycles	7	5	12	1	1
Average p-cycle size	7.9	10	9.2	14	14
Working capacity	840	880	994	1120	1120
Spare capacity	740	668	658	560	560
Redundancy	88%	76%	67%	50%	50%
Protection gap ratio	12%	15%	2.9%	0%	0%
Protection overhead ratio	12%	0.3%	5.5%	0%	0%

Table 5.4: CG vs. Conventional Design Methods of PWCE - NSF Network

The number of selected p-cycles corresponds to the number of activated p-cycles in the optimal solution, these numbers are remarkably smaller than the set of considered potential p-cycles in the B-ILP method. These numbers in the B-ILP approach are far from the initially considered potential p-cycles in all the considered networks. Our optimization objective is to maximize the size of the protected working capacity envelope. Note that the selected p-cycles with a larger average size (row 3) in B-ILP are globally more efficient than those of S-ILP, E-ILP and G-ILP.

	COST239				
	S-ILP	E-ILP	G-ILP	B-ILP	CG
# of potential p-cycles	26	97	763	3517	3
Computing time (sec.)	0.02	0.08	0.42	21.5	0.03
# of selected p-cycles	19	25	19	1	1
Average p-cycles size	4.5	6.1	6.95	11	11
Working capacity	1120	1292	1472	1640	1640
Spare capacity	858	788	608	440	440
Redundancy	76%	61%	41.3%	26.8%	26.8%
Protection gap ratio	9.2%	0%	0%	0%	0%
Protection overhead ratio	15.4%	1.3%	5.3%	0%	0%

Table 5.5: CG vs. Conventional Design Methods of PWCE - COST239 Network

The size of the resulting PWCE is proportional to the size of the considered p-cycles in the final solutions of all evaluated methods. The activated p-cycles in the optimal solutions of S-ILP. E-ILP and G-ILP are slightly smaller, require more spare capacity and provide less protected working capacity, and thus, result in high protection redundancy. Two more characteristics of S-ILP, E-ILP and G-ILP are: They do not provide 100% protection in the network, and some protection capacity is useless (overhead) along some links. Protection gap ratios of up to 12%. 15% and 3% and protection overhead ratios of up to 15.4%, 8.8% and 9.% are recorded with S-ILP, E-ILP and G-ILP, respectively.

	USA				
	S-ILP	E-ILP	G-ILP	B-ILP	CG
# of potential p-cycles	35	96	1017	7314	3
Computing time (sec.)	0.03	0.05	0.64	190	0.2
# of selected p-cycles	19	17	18	1	1
Average p-cycles size	6.7	8.36	12.38	28	28
Working capacity	1916	2045	2308	2480	2480
Spare capacity	1604	1501	1264	1120	1120
Redundancy	83.7%	73.4%	54.8%	45%	45%
Protection gap ratio	4.2%	2.7%	1.3%	0%	0%
Protection overhead ratio	11.3%	8.8%	9.5%	0%	0%

Table 5.6: CG vs. Conventional Design Methods of PWCE - USA Network

Although the S-ILP, E-ILP and G-ILP solutions are less time consuming than those based on B-ILP solutions, they are not as capacity efficient as the B-ILP solutions are. The protected working capacity and the required spare capacity of these former solutions are far less efficient than the optimal solutions of the B-ILP method.

Table 5.7 summarizes the results of the previous experiments obtained by the S-ILP, E-ILP and G-ILP methods. The capacity gap to the optimality, which we define as the redundancy + protection gap + protection overhead, shows the poor quality of the deployment obtained by the inherent methods.

	S-ILP	E-ILP	G-ILP
NSF	62%	41.3%	25.4%
COST239	73.8%	35.5%	19.8%
USA	54.2%	39.9%	20.6%

Table 5.7: Optimality Gap of S-ILP, E-ILP and G-ILP

Our CG-based design approach of p-cycle-based PWCE gathers the two qualities of the previously analyzed approaches, namely, the efficiency of the B-ILP method and the scalability (computing

	France			Brazil		
	G-ILP	B-ILP	CG	G-ILP	B-ILP	CG
# of potential p-cycles	2263	-	2	4613	-	2
Computing time (sec)	4.15	-	0.6	45.5	-	6.6
# of selected p-cycles	44	-	1	51	-	1
Average p-cycles size	16	-	43	11	-	27
Working capacity	3625	-	3960	3961	-	4520
Spare capacity	2011	-	1720	1627	-	1080
Redundancy	55.5%	-	43%	41%	-	23%
Protection gap ratio	1.21%	-	0%	0.3%	-	0%
Protection overhead ratio	4.3%	-	0%	10.1%	-	0%

Table 5.8· CG vs. Conventional Design Methods of PWCE - Larger Networks

time) of the S-ILP, E-ILP and G-ILP. Regardless of the size of the network, our CG method generates a limited number of p-cycles (3 in all cases), among the most relevant, and selects only what is needed (1 Hamiltonian p-cycle in all cases). In contrast to B-ILP, our optimization model is highly compact (generates less potential p-cycles) and results in significantly less resource usage (runtime is 1000 times less than the B-ILP approach). Moreover, if we focus closely on the computing times, it is clear that our CG-based approach is not only faster than the B-ILP, but also faster than some of the other evaluated compact approaches, i.e., S-ILP, E-ILP and G-ILP.

In the second category of experiments, larger network instances are considered (the last two networks in Table 5.2). The objective of these experiments is to evaluate the scalability of our design approach on larger network instances. The results obtained by our CG-based approach, the G-ILP and B-ILP approaches (more capacity efficient methods) are shown in Table 5.8. As in the previous experiments, the G-ILP approach is fast in combining the limited number of p-cycles in interesting solutions. However, its redundancy is still high ($\sim$ 20% more than the CG-based approach). In these two networks, the B-ILP approach fails to find a solution for the problem· No interesting solution has been found within the runtime of the solution method (6 days). Our CG-based approach is by far the best approach for these two large networks. it is faster than the G-ILP approach and provides the optimal solution for the design problem The average size of the activated

p-cycles in these last experiments and all the previous ones is larger in the optimal solution, which allows us to conclude that, for PWCE design, larger p-cycles are more efficient than smaller. In addition to its capacity efficiency and scalability, our CG-based approach activates a small number of p-cycles in order to guarantee 100% protection (protection gap =0). Regarding the deployment issue of the p-cycles generated by the previously studied methods, the CG-based approach and the B-ILP (but B-ILP is not scalable) provide the easiest and practical solutions. Indeed, as the number of activated p-cycles is small, their deployment in a wavelength switched network (no wavelength conversion) becomes easier than with a larger number of p-cycles in the other approaches, i.e, S-ILP, E-ILP and G-ILP (need to solve another hard wavelength assignment problem).

We have performed other experiments to show the limitations of the explicit enumeration of all the p-cycles before the optimization process. In the two-step approach, the p-cycle enumeration process is done ahead of the optimization process, only the physical connectivity of the networks is considered at this stage. We have varied the number of wavelength-channels of the physical links in the network, two capacity intervals ([40-80] and [60-80]) have been selected and a uniform distribution of link capacity was applied in these intervals, see Table 5.9. Intuitively, as the physical topology remains unchanged, the size of the set of enumerated p-cycles remains the same in the two-step methods, though, links with few channels (bottleneck links) and those with large number of channels will be used equally as in the case of links with the same capacity In our CG-based approach, p-cycles are generated by the pricing problem based on the dual variables of the master problem, the so far available capacity on each link is coded by these variables. So, the p-cycle generation process is dynamically adapted to the current available capacity.

Table 5 9 gives a strong insight on the limitation of the two-step methods (either based on extensive or selected p-cycle enumeration). With links of different capacities. the active set of p-cycles in the optimal solution grows as the capacity interval is extended. The active set of p-cycles is a bit larger than in the case where links are of the same capacity, (4 to 7) for B-ILP and CG-based approach The computing times of the CG-based solution method are by far the best of all the computing times of the other methods. We solved the same ILP models as in the previous set

	COST239					
	[40-80]			[60-80]		
	G-ILP	B-ILP	CG	G-ILP	B-ILP	CG
# of potential p-cycles	763	3517	7	763	3517	14
Computing time (sec)	1256	1846	8.4	1722	128	21.55
# of selected p-cycles	17	7	6	19	4	6
Average p-cycles size	6.5	7.43	8.67	6.84	8	8.33
Working capacity	1010	1056	1056	1303	1429	1429
Spare capacity	442	390	384	550	426	426
Redundancy	44%	37%	36.3%	43%	30%	30%
Protection gap ratio	0%	0.5%	1.2%	0.3%	0.1%	0.1%
Protection overhead ratio	18%	64%	55.7%	13%	28%	22%

Table 5.9: CG vs. Conventional Design Methods of PWCE - Links with Different Capacities

of experiments (different transport capacities along links). on all the five networks considered in this study, and the obtained results were similar to the ones presented in Table 5.9, i.e, CG-based approach was by far the most efficient and scalable method among all the studied methods. The two solutions given by the B-ILP and CG-based methods in these two experiments have the same value (same PWCE size), although their redundancy, protection gap and protection overhead ratios are a bit different. The objective is to maximize the number of protected working channels in the network, so the working capacity envelope is of the same size in both cases, but its shape is not (not the same number of selected p-cycles in both methods). Different planning of spare capacity can create different PWCE shapes. In Table 5.9 the protection gap of the CG-based solution method is greater than that of B-ILP, but the protection overhead of the CG-based method is less than that of B-ILP. The difference between the two protection gap ratios is used as protection capacity in the B-ILP method (398 channels vs. 384 in CG-based approach), while the CG-based approach keeps it as unprotected capacity. The unprotected capacity (protection gap) of both methods is still usable to carry unprotected traffic. thus the CG-based approach provides more working (even unprotected) capacity than the B-ILP method. Based on the above remarks, the solutions obtained with our CG-based approach are better than those provided by the B-ILP method, even though they provide

PWCEs of the same size.

5.6 Non-Simple p-Cycle Numerical Results

In this section, we evaluate the added value in terms of protection performances of non-simple p-cycles over simple p-cycles. Recall that the simple p-cycle set is a subset of the non-simple p-cycle one. In this part of the numerical results, we focus on varying the link spare capacity budget, and see how the capacity redundancy ratio and the reliability ratio (, i.e., the ratio of protected capacity over the sum of the protected and non protected capacities) vary accordingly. We have summarized in Figure 5.6 the variation of these two ratios depending on the link spare capacity budget, for all four network instances.

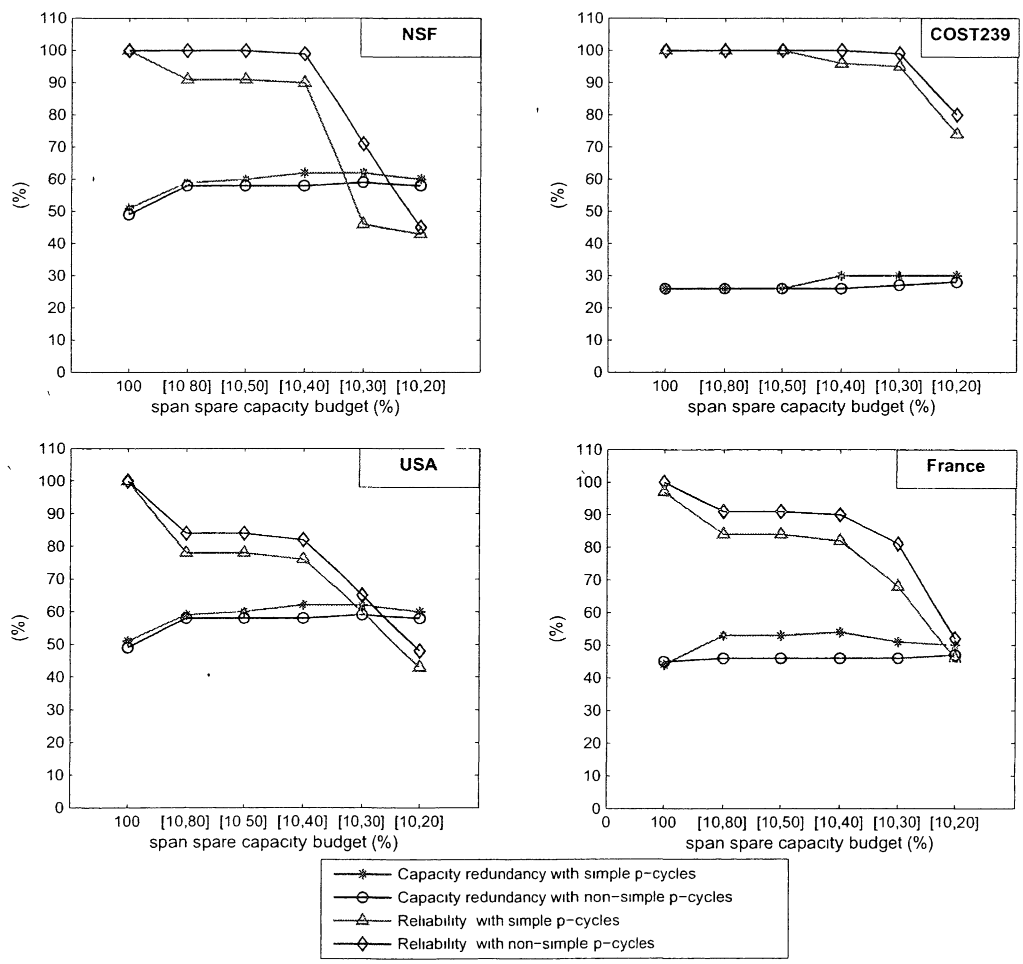


Figure 5.6: Non-Simple vs. Simple p-Cycle Protection Performances

The X-axis indicates the link spare capacity budget (upper bound on the link protection capacity), where 100% means that the potential spare capacity is equal to the total link transport capacity, and $[i, j]$ that the link spare capacity budget lies in the interval $[i, j]$ of the total transport capacity. We have considered six intervals of link spare capacity (see Figure 5.6) budget and applied uniform distributions of spare capacity over links in all the considered intervals.

The capacity redundancy of the simple p-cycle based PWCE design method is higher than that based on non-simple p-cycle one in all the experiments that we conducted. When no limit is imposed on the link spare capacity budget (100% of transport capacity can be used as protection capacity on all links), the simple p-cycle based PWCE design method almost achieves the same capacity redundancy and reliability as the non-simple p-cycle based method. However, when the available link spare capacity budget is reduced, the non-simple p-cycle based PWCE method becomes more efficient (less capacity redundant and more reliable) than the simple p-cycle based method. This difference is more apparent in the France, USA and NSF networks and less in COST239 network: the design method based on non-simple p-cycles is $\sim$ 25% more reliable for the NSF network (link spare capacity in [10,30]) than the method based only on simple p-cycles. Regarding the capacity redundancy, the design method based on non-simple p-cycles is $\sim$ 10% less capacity redundant in the France network than the method based only on simple p-cycles.

We observe that there is one network topology. the COST 239, for which almost similar performances are obtained with the simple and the non-simple p-cycles. By having a close look to the characteristics of the topologies, we observe that COST239 has a high connectivity for all its nodes (low σ), and therefore high flexibility is possible, whenever we set simple or non-simple p-cycles. The NSF network has lower connectivity (sparse network) and the degree values are widely spread (high σ). Reducing the link spare capacity budget along some chosen links can reduce considerably the capacity efficiency of the design method using simple p-cycles. Non simple p-cycles offer more flexibility in exploiting the spare capacity, therefore they are more efficient than simple ones in using it, especially when it comes to building the PWCE in sparse networks. While the USA and France networks have similar average degrees, they have different degree standard deviations, see Table 5.2:

42% of the nodes in France network have a degree ≥ 4 compared to 35% in the USA network. These characteristics explain why the advantage of using non-simple p-cycles rather than simple ones, is most apparent in the France network.

In order to better assess the advantage of the non-simple over the simple p-cycles with respect to the variability of the connectivity parameters, or more generally, with respect to the variability of the spare capacities on the links, we decided to perform some additional experiments where we considered different distributions of the link spare capacity budget so as to artificially increase the node degree discrepancies. We, therefore, modified the link spare capacities so as to set $\sim$ 10% of them to 0, in other words, to have 10 % of the links with a spare capacity budget equal to 0. Results are reported in Figure 5.7. The advantage of non-simple p-cycles over simple ones increases with the node degree discrepancies.

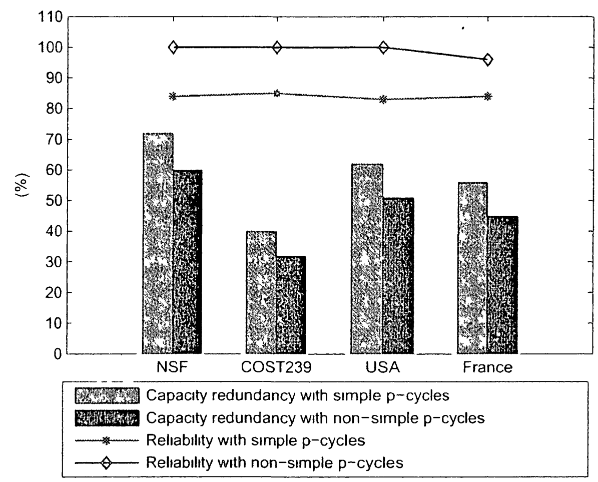


Figure 5.7: Node Degree Discrepancy Effect on p-Cycle Protection Capabilities

More generally, as the set of non-simple p-cycles is much larger than the set of simple p-cycles, a PWCE design with non-simple p-cycles will always be at least as good as a PWCE design with simple p-cycles, independently of the spare capacity distribution and the network connectivity.

5.7 Conclusion

The objective of this work was to develop a scalable and efficient method for the design of survivable WDM networks based on p-cycle-PWCE without a priori enumeration of any p-cycle. We first, using a column generation (CG) technique, developed a very efficient and scalable approach based on simple p-cycles where we focus on performance analysis, and secondly, extended the approach to include non-simple p-cycles as well as simple p-cycles.

Unlike classical design methods of survivable WDM based on p-cycle-PWCE, our CG-based model and solution method does not require any prior enumeration of p-cycles, globally relevant cycles are dynamically generated during the optimization process based on the link spare capacity budget and the protection needs.

To show the effectiveness of our CG-based method with simple p-cycles, we conducted extensive computational experiments on a set of five networks with different topology shapes. Results show that solutions of our CG-based method are much better than the solutions of all previously proposed methods within different design conditions. Further results showing the advantages of using non-simple p-cycles over simple ones in the design of PWCEs were presented especially in sparse networks and with non homogeneous link spare capacity budget.

CHAPTER 6

The Pre-configured Protection Extended-Tree Scheme

6.1 Introduction

Migration from ring-based towards mesh-based network architectures has raised many problems in the design and operation of optical networks and opened up several research directions. In the design of protection schemes, mesh-based architectures offer higher flexibility in the configuration of protection planes by enabling richer connectivity than ring-based ones. Though, a variety of shared protection topologies with different protection performances including, for example, cycles, trees, and linear trails can be deployed to provide protection in contrast to ring architectures where the network topology limits the candidate protection topologies to rings.

The design problem of protection schemes in mesh optical networks involves different protection parameters, and a variety of design constraints and objectives. Different trade-offs exist among the different parameters in the design of protection schemes. The recovery delay and protection capacity cost are among the most targeted design parameters in different design approaches. The protection performance of a global scheme depends on the shape of its protection building blocks (logical topologies). Direct deployment of ring structures in mesh networks has been shown not to be efficient and requires high protection capacity [EHS00]. The p-cycle-based approach [GS98] has been proposed as a solution to deployment of cyclical structures in mesh networks. This approach preserves the advantage of ring topologies in terms of recovery delay, and extends their protection capacity efficiency by enabling protection of straddling-cycle links. The high speed recovery delay of ring and p-cycle-based schemes is not really due to their ring-like topology. Rather, it is due to the fact that the protection capacity can be fully configured ahead of any failure, and used with a limited reconfiguration in case of a failure. Indeed, the pre-cross connectivity of these protection topologies allows dynamic monitoring and tuning of optical signals, though, guarantees high integrity of the backup paths before any traffic switching. This property is very important, especially in *transparent* optical networks. The pre-cross connectivity imposes a specific sharing strategy that may affect the cost of the required spare capacity in order to yield a 100% protection in a network. In addition, to be efficient, some fully pre-cross connected structures, e.g , p-cycles, may require a specific spare capacity distribution over the network links (see Section 3.5).

Another protection topology in mesh networks that can enable interesting protection features is the pre-configured protection tree (p-tree) scheme. It is a highly scalable and a flexible structure that can support larger failure scenarios, such as, recovery from multiple failures. Dynamic provisioning of protection capacity with p-trees can be performed incrementally by local extensions of a p-tree (adding branches). Although p-tree-based protection offers the advantages of scalability, local restoration capabilities, and failure impact restriction, it suffers from capacity inefficiency [GG07] and recovery delay due to the dynamic cross connection of the protection capacity.

In this chapter, we propose a novel protection approach named *pre-configured protection extended-tree (p-etree)*. This novel protection approach uses hybrid protection structures based on p-trees and p-cycles. In Section 6 2, we give our motivation and goals for the p-etree scheme. We present more in detail the concept of p-etree in Section 6.3, and propose an optimization model based on CG in order to optimize the size and shape of different PWCEs in Section 6.4 Section 6.5 contains the computational results. Therein, we evaluate the capacity efficiency and the recovery delay of the p-etree scheme and compare its performance with different pre-defined shape structure based protection schemes. Different link spare capacity budgets are used to measure the flexibility of the compared methods. Section 6.6 concludes the chapter.

6.2 Motivation and Goals

In this chapter, we are interested in the design of protection schemes where the link spare capacity budget is not uniform, and the protection topologies are not all of the same shape and type. Our main concern is to develop flexible and scalable structures to provide the expected protection level with the lowest possible spare capacity budget and an optimized recovery time when the link spare capacity budget is not necessarily uniform. The p-cycle and p-tree structures belong to two different families of protection structures: The fully pre-cross connected and dynamically cross connected structures. These two complementary structures can be used to supply their mutual needs and offset their mutual disadvantages. Indeed, the capacity efficiency of p-cycles and their recovery delay can offset the capacity inefficiency and recovery delay of p-trees. and the scalability and flexibility of p-trees can offset that of p-cycles. Based on these two pre-defined shape protection structures, we propose a novel protection strategy that consists to potentially construct fully pre-cross connected structures such as p-cycles and p-trails, starting from a p-tree by re-shaping its topology. Our goal is to construct scalable protection structures from basic p-trees by potentially (when it is profitable and there is enough spare capacity) extending their protection capabilities and optimizing their recovery delays. We establish some new integer linear programming models, and use CG in order to optimize the construction of the p-etree structures in the design of PWCEs.

6.3 The Pre-Configured Extended-Tree (p-eTree) Concept

In the design of protection schemes, we are used to approaches, which consist to name the protection scheme after the shape of the protection topologies, e.g., p-cycle and p-tree based protection schemes. The protection performance including capacity efficiency, recovery delay, flexibility and scalability of those protection schemes depend greatly on the shape of the protection structures Hence, at a certain degree, we can predict the performance of a global scheme if we know the shape of the protection building blocks. In the next section, we present an illustrative example of the p-etree construction in a network model where the link spare capacity is not uniform and p-tree and p-cycle schemes are either not efficient or not flexible in providing the targeted protection. Therein, we discuss in detail the p-etree protection scheme and its potential building blocks.

6.3.1 Toward the p-eTree Scheme

Figure 6.1 presents a WDM network $G(\mathcal{V}, \mathcal{L})$ where a link spare capacity budget is given next to each link as follows: each link ($\ell \in \mathcal{L}$) has two units of spare capacity except links $\ell_{E,F}$ and $\ell_{E,D}$ which have no available spare capacity (equal to zero). We assume that the objective is to maximize

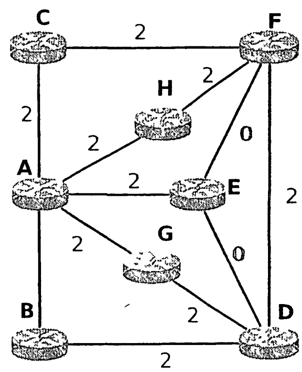


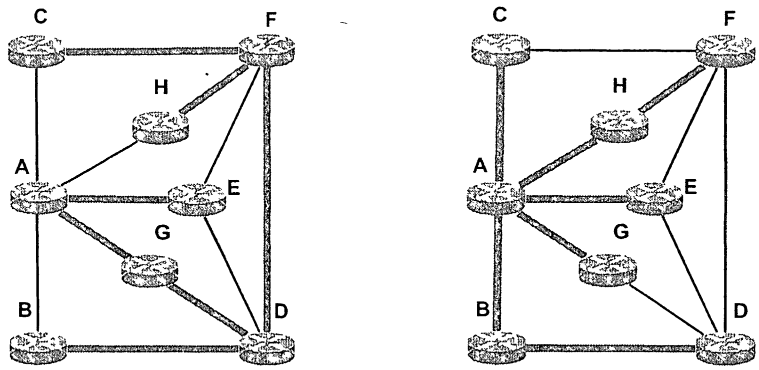
Figure 6.1: Spare Capacity Model

the size of the PWCE, i.e., protect the maximum possible amount of capacity. In the next three sections, we illustrate three optimal designs of protection schemes respectively based on p-trees, p-cycles and p-etrees and compare their designs of PWCEs.

Pre-configured Protection Tree (p-Tree) Scheme

The basic building blocks in p-tree protection schemes [SG99] are trees. A pre-configured tree (p-tree) can provide protection only for straddling-tree links (links whose two-end nodes are in the same tree, but do not define a tree link). In order to ensure efficient protection, multiple overlapping p-trees are required. Figure 6.2 illustrates an optimal p-tree based scheme where two overlapping trees on different channels provide protection in the network model of Figure 6.1. In terms of capacity efficiency, p-tree based protection is known to be far less capacity efficient than the p-cycle protection [GG07]. In addition, as a basic protection pattern, a p-tree cannot be considered as a totally pre-cross connected structure, unless, it is shaped like a linear trail (no bifurcation).

However, the p-tree protection has some advantages over linear and cyclical protections. Firstly, when spare capacity is not uniformly distributed over the links of a network, cyclical structures like p-cycles may not be able to economically provide a given protection level [HS07]. Secondly, in case of a failure, it is possible to perform local restoration through dynamic cross connection of some backup segment paths. These advantages allow more flexibility in exploiting the spare capacity, and thus increases the resiliency against multiple failures, even if the protection scheme aims at only addressing the single failure protection issue. Through dynamic cross-connection of spare capacity at nodes F and D in Figure 6.2-(a) and at node A in Figure 6.2-(b) it is possible to restore any one of the straddling-tree links even those without spare capacity.



(a) (b)

Figure 6.2: Pre-Configured Protection Tree (p-Tree) Scheme

Although the flexibility in provisioning protection capacity is higher when the cross connects are made dynamically, the delay incurred by the dynamic setting of the paths (particularly when many sequential cross-connects need to be set up on the fly) may seriously slow down the dynamic provisioning operation, especially in transparent networks.

Pre-Configured Protection Cycle (p-Cycle) Scheme

The p-cycle protection scheme [GS98] is widely acknowledged as the most efficient pre-configured protection scheme in terms of capacity efficiency and switching delay [SG00]. However, when the distribution of spare capacity over the links is not uniform, or in case of a sparse network, setting up a p-cycle may result in an expensive investment in terms of spare capacity [HS07].

In Figures 6.3-(a) and 6.3-(b), two optimal designs based on simple and non-simple p-cycles respectively are illustrated of the network model in Figure 6.1. Each of the simple p-cycles in Figure 6.3-(a) has one capacity unit while in Figure 6.3-(b) the single non-simple p-cycle has two capacity units. Compared to the previous p-tree design, which uses 14 spare channels and provides only 10 protected channels, the two simple and non-simple p-cycle-based schemes use 18 and 16 channels, and provide respectively 18 and 20 channels.

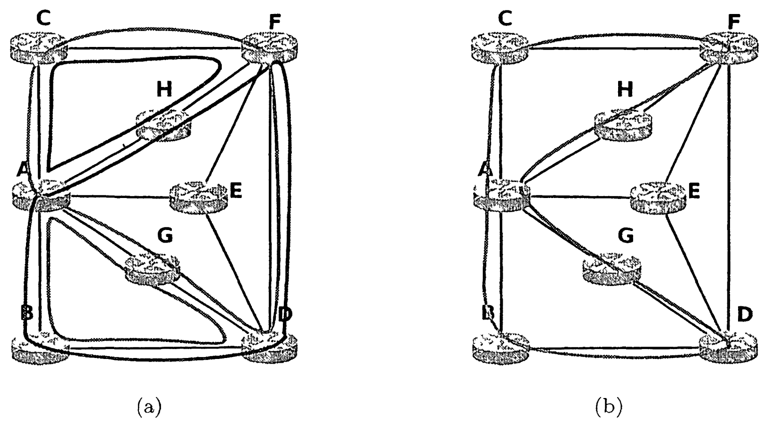


Figure 6.3: Pre-configured protection Cycle (p-Cycle) Scheme

Due to the link spare capacity budget constraint, none of the totally pre-cross connected cyclical structures can provide protected capacity on links $E-F$ and $E-D$. Existing solutions in the literature which consist to combine totally pre-cross connected patterns like p-cycles and linear trails [SG99. LS08] cannot remedy the problem in this case without affecting the capacity efficiency of the protection scheme.

Pre-configured Protection Extended-Tree (p-eTree) Scheme

Our proposal for pre-configured extended-trees is motivated, on the one hand, by the capacity efficiency and restoration speed of p-cycle schemes and, on the other hand, by the flexibility of p-trees and linear trails in providing protected capacity even within constrained spare capacity budgets.

Figure 6 4 illustrates a p-etree protection scheme in the network model of Figure 6.1. We use two copies of the illustrated p-etree structure The bold lines represent the basic tree. and the dashed bold lines the extending tree links. The resulting structure is a hybrid one, composed of two sub structures: A pre-cross connected (cyclical thick lines), and a linear trail which is incident to the first one, but not a priori cross-connected with it (link $E - A$).

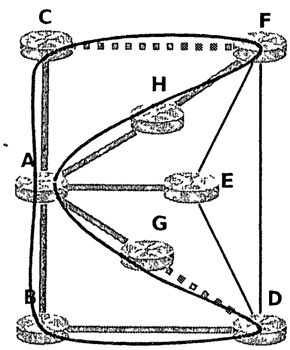


Figure 6.4: Pre-Configured Extended-Tree (p-eTree) Scheme

In Figure 6.4, the selected tree (not necessarily a spanning tree) is extended by adding some straddling-tree links $C - F$ and $G - D$ and cross-connecting the spare capacity at node A as follows: $A - C$ connected to $A - B$, $A - H$ connected to $A - G$. The resulting pattern is an optimized pre-cross connected structure where, only a limited number of cross-connects need to be performed dynamically in case of a failure In Figure 6.4, only node A needs to perform dynamic cross-connection of protection capacity in case of a failure, and this is only when a failure occurs on link $E - F$ or $E - D$. The protection branch $A - E$ incident at the non-simple p-cycle structure is part of the initial p-tree and it is part of the current p-etree. In case of a failure on link $E - F$ or $E - D$, this branch is connected to $A - H$ or $A - G$ in order to isolate the backup path to protect $E - F$ or $E - D$ respectively

Let us have a look at the capacity efficiency of our p-etree protection scheme in Figure 6.4: Therein, we use 18 spare channels and provide 24 protected channels, i.e., more protected channels compared to the previous p-tree and p-cycle scheme in Figures 6.2 and 6.3, respectively. Moreover, the capacity redundancy of the p-etree scheme is 0 75 whereas it is 0.8 and 0 9 for the non-simple and simple p-cycle schemes, respectively.

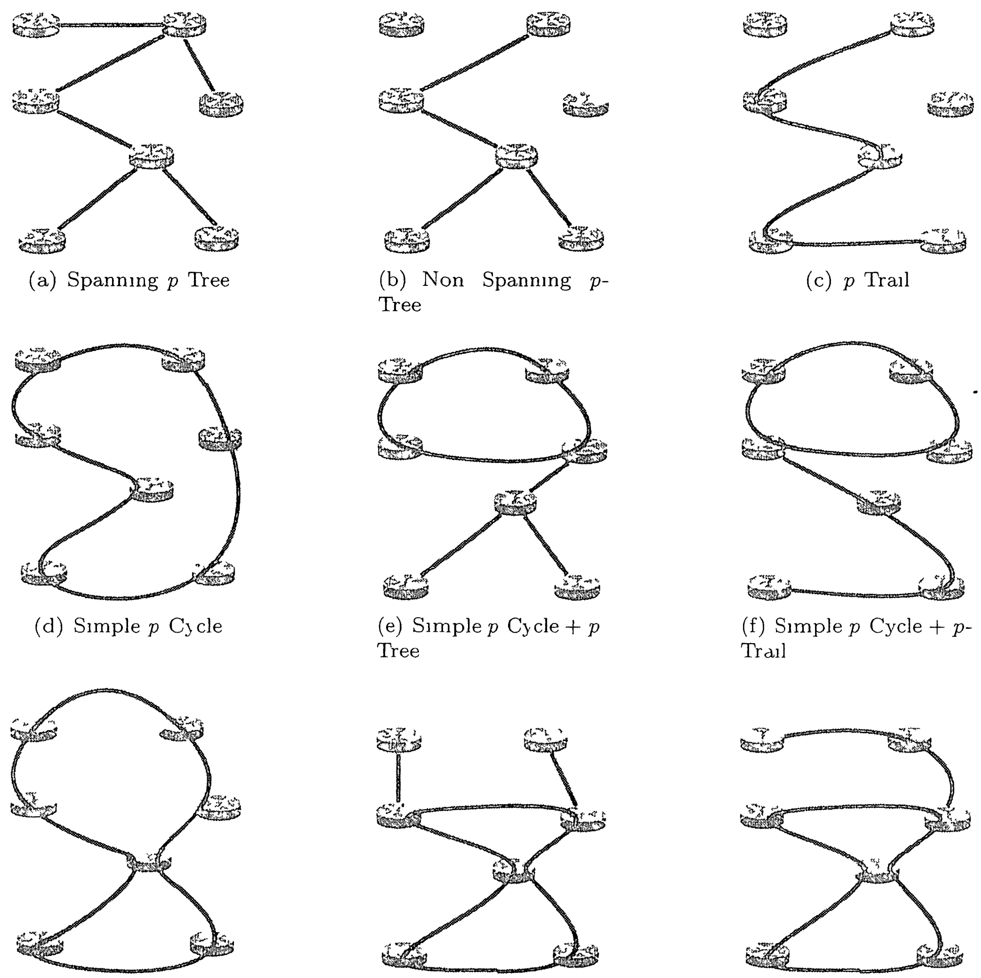
In Figure 6 4. a potential protection structure of the p-etree protection scheme is illustrated. However. following the extension strategy. different other shapes can result. In the next section. we illustrate other potential p-etree structures.

6.3.2 Potential p-eTree Protection Structures

There is a priori no restriction on the shape of the building blocks in a p-etree scheme. Starting from a tree, we can construct different shape structures including simple and non-simple cycles, trails, and a bunch of hybrid structures composed of elementary cycles, trails, and trees. In Figure 6.5, we represent all the potential shapes that can take the protection structures resulting from extending p-trees following the p-etree approach. The protection structures can be classified into two families:

- Pure structures, which include pure p-trees (spanning all the network nodes or not), see Figures 6.5-(a),(b), pure p-trails in Figures 6.5-(c), pure simple p-cycles, see Figures 6.5-(d), and pure non-simple p-cycles, see Figures 6.5-(g). Recall that a p-trail is a particular p-tree without bifurcations, and a simple as well as a non-simple p-cycle can be obtained from a p-tree by adding one and two straddling-tree links, respectively.
- Hybrid structures, this family can be divided into two sub-families
  - Hybrid p-cycles and p-trees, includes simple as well as non simple p-cycles combined with p-trees, see Figures 6.5-(e) for simple p-cycles and Figure 6.5-(h) for non-simple p-cycles.
  - Hybrid p-cycles and p-trails, includes simple as well as non simple p-cycles combined with p-trails, see Figures 6.5-(f) for simple p-cycles and Figure 6.5-(i) for non-simple p-cycles.

The p-etree design approach extends the solution space of all previously proposed schemes with pure and hybrid patterns. Though. it is more flexible to meet different objectives in the design problem. In Figures 6.2 to 6.4, the design objective is to maximize the size of the PWCE. However, with the extended range of potential protection structures in the p-etree approach, different other design objectives can be effectively reached.



(a) Spanning p Tree (b) Non Spanning p-Tree (c) p Trail

(d) Simple p Cycle (e) Simple p Cycle + p Tree (f) Simple p Cycle + p-Trail

(g) Non Simle p Cycle (h) Non-Simle p Cycle + p-Trees (i) Non Simle p Cycle + p Trail

Figure 6 5 Potential (p-eTree) Protection Structures

6.3.3 Recovery Delay Analysis of p-eTree Scheme

Regarding the recovery delay the resulting *optimized pre-cross connected* p-etree structures can approach the speed of a totally pre-cross connected structure Indeed, when signaling messages to set up the cross-connects are sent out-of-band to a very limited number of nodes, it is possible to set up these cross-connects in parallel with those at the end-nodes of the affected link In order to discuss the recovery delay, we introduce the following notation

- D_n Time for a node n to detect a link failure on one of its incident links
- P_ℓ Propagation delay on link ℓ

- T_n: Time to process and transmit a message at node n.

- C_n: Time to setup and test a cross-connect at node n ($C_n > T_n + P_\ell$).

In order to simplify the analysis, we assume that setting and testing a cross connect takes the same amount of time at all the nodes ($C_n = C$), and that signaling is performed sequentially along the backup protection paths. Thus, the recovery delay in case of a hybrid or pure protection pattern is equal to:

$$D_s + T_1 + P_{\ell_1} + T_2 + P_{\ell_2} + \cdots + C = D_s + \sum_{i=1}^{h} (T_i + P_{\ell_i}) + C, \qquad (6.1)$$

where h is the number of nodes along the backup path that are sent a request to setup the backup path (can be half of the nodes when the two end-nodes participate in the recovery process). As setting up and testing cross connects at intermediate nodes are performed in parallel with message transmission and propagation, we do not include their incurred delay in the recovery delay formula.

The recovery delay in formula (6.1) is sensitive to the number of intermediate unset cross-connects. When there is none (totally pre-cross connected pattern), the recover delay becomes the same as in a totally pre-cross connected pattern, i.e., $D_n + C$. With a p-etree protection, we can maximize the protected working capacity. and implicitly the number of pre-cross connected backup paths. In Figure 6.4, the failure of any of the links which is part of the cyclical layout will require a recovery delay of $D_n + C$, and the off-cyclical layout link $E - A$ a recovery delay of $D_n + P_1 + T_1 + C \simeq D_n + C$. i.e.. the recovery time of a totally pre-cross connected structure.

6.4 Optimized Design of p-eTree Protection Scheme

In this section. we propose an optimization model based on CG in order to optimize the selection of p-etree in the design of a maximized size PWCE. Same optimization and decomposition approaches as in Chapter 5 are used in this chapter The only difference is the shape of protection building blocks. In this chapter. we use p-etrees while in Chapter 5 we used p-cycles. Though. we re-use the master problem of p-cycle based scheme in Section 5.4.1. and update the pricing problem in order to re-shape the potential protection structures. Using the values of the dual variables of the master problem, which code the information about spare capacity availability and protection needs, the pricing problem generates a new potential p-etree at each iteration.

The expression of the pricing objective, i.e., the maximization of the reduced cost is not different from that of the p-cycle based approach. The only difference is parameters a_ℓ which are associated with a different expression in the p-etree approach. Indeed, for each link ℓ, in the p-cycle scheme, a link cannot be granted more than 2 protection paths by any given p-cycle ($a_\ell \in \{0, 1, 2\}$), while in the p-etree scheme this value can theoretically grow up to the maximum number ≥ 2 of backup paths a p-etree can provide for a link. The pricing objective is written as follows:

$$\max \left(\sum_{\ell \in L} \theta_\ell^1 a_\ell^s - \sum_{\ell \in L} \left(\theta_\ell^2 + \theta_\ell^3 \right) b_\ell^s \right),$$

where θ_ℓ^1, θ_ℓ^2 and θ_ℓ^3 are the dual variables associated with constraints (5.1), (5.2) and (5.3), respectively.

The pricing problem generates pre-configured extended-tree (p-etree) structures to protect link-channels in the network. To ease the presentation, we start by presenting the pure p-tree optimization problem before we move to the added extension and the whole p-etree.

6.4.1 p-Tree Construction

We define the variables of the pricing problem used in shaping the p-tree $\mathcal{T}$ as follows:

$$r^{v_i} = \begin{cases} 1 & \text{if } v_i \text{ is the root-node of } \mathcal{T} \\ 0 & \text{otherwise,} \end{cases}$$

$$y_{v_i}^{v_j} = \begin{cases} 1 & \text{if node } v_j \text{ is the parent node of node } v_i \\ 0 & \text{otherwise,} \end{cases}$$

$$x_\ell^{\mathcal{T}} = \begin{cases} 1 & \text{if link } \ell \text{ is a straddling-}\mathcal{T}\text{ link} \\ 0 & \text{otherwise.} \end{cases}$$

The constraints of the sub pricing problem (only the p-tree construction) are defined in order to generate a single tree (not necessarily a spanning tree) at each iteration.

$$\sum_{i \in N} r^{v_i} = 1 \tag{6.2}$$

$$\sum_{v_j \in \mathcal{V}(i)} y_{v_i}^{v_j} + r^{v_i} \leq 1 \qquad v_i \in \mathcal{V} \tag{6.3}$$

$$x_\ell^{\mathcal{T}} + y_{v_j}^{v_i} + y_{v_i}^{v_j} \leq 1 \qquad \ell = \{v_i, v_j\} \in \mathcal{L} \tag{6.4}$$

$$2x_\ell^{\mathcal{T}} \leq \sum_{v_i \in \mathcal{V}(\ell)} \left(\sum_{v_k \in \mathcal{V}(v_i) \setminus \mathcal{V}(\ell)} y_{v_i}^{v_k} + r^{v_i} \right) \qquad \ell \in \mathcal{L} \tag{6.5}$$

$$\sum_{v_i, v_j \in N} (y_{v_i}^{v_j} + y_{v_j}^{v_i}) \leq |N| - 1 \qquad N \subset \mathcal{V}, v_i, v_j \in N \tag{6.6}$$

$$x_\ell^{\mathcal{T}}, y_{v_i}^{v_j}, r^{v_i} \in \{0, 1\} \qquad \ell \in \mathcal{L},\ v_i, v_j \in \mathcal{V}. \tag{6.7}$$

Constraint (6.2) identifies the root-node (one root-node). Constraints (6.3) select one parent in the p-tree for each node that is not a root-node. Constraints (6.4) prevent cycling on a parent-son relationship (at most $y_{v_j}^{v_i}$ or y_i^j equal to 1) if ℓ is not a straddling-tree link. Constraints (6.5) stipulate the necessary conditions for a link to be a straddling-tree link, i.e.. each of its end-nodes should have a parent in the tree if it is not the root-node. Constraints (6.6) prevent unconnected components from arising in the network. e.g., under the form of cycles. These constraints are not all enumerated. rather they are added only when they are violated Constraints (6.7) enforce the integrality of the variables.

6.4.2 p-Tree Reshaping

So far, we have built a p-tree. Let us extend the p-tree structure to build p-etree structures. The following variables are used to reshape the tree and count the number of alternative backup paths for each link ℓ. By extending the selected tree, we aim at forming an optimized pre-cross connected structure (p-cycles), but some branches of the tree may not be part of it.

$$x_\ell^{\mathcal{OXC}} = \begin{cases} 1 & \text{if } v_i \text{ belongs to the pre-cross connected part of the current } p\text{-etree} \\ 0 & \text{otherwise,} \end{cases}$$

$$x_\ell^{\mathcal{BCK}} = \text{number of disjoint backup paths for link } \ell$$

Constraints of the second part of the pricing are as follows:

$$x_\ell^{\mathcal{OXC}} \leq x_\ell^{\mathcal{T}} + y_{v_j}^{v_i} + y_{v_i}^{v_j} \qquad \ell = \{v_i, v_j\} \in \mathcal{L} \tag{6.8}$$

$$\sum_{\ell \in \mathcal{E}(v_i)} x_\ell^{\mathcal{OXC}} = 2n_{v_i} \qquad v_i \in \mathcal{V} \tag{6.9}$$

$$x_\ell^{\mathcal{BCK}} \leq \sum_{\ell' \neq \ell, \ell' \in \mathcal{E}(v_i)} x_{\ell'}^{\mathcal{OXC}} \qquad v_i \in \mathcal{V}, \ell'. \ell \in \mathcal{L} \tag{6.10}$$

$$x_\ell^{\mathcal{BCK}} \leq \sum_{\ell' \in \mathcal{E}(N)} x_{\ell'}^{\mathcal{OXC}} \qquad N \subset V, \ell \in \mathcal{L} \tag{6.11}$$

$$x_\ell^{\mathcal{OXC}} \in \{0,1\}, x_\ell^{\mathcal{BCK}}, n_{v_i} \in \mathbb{Z}^+ \quad \ell \in \mathcal{L}, v_i \in \mathcal{V} \tag{6 12}$$

Constraints (6.8) restrict the extensions to either on-tree or straddling-tree links, in order to define a p-etree structure. Constraints (6.9) guarantee that the pre-cross connected structure will involve nodes with an even degree (Eulerian tour). Constraints (6.10) are used to count the number of alternative backup paths for each link in the pre-cross connected p-etree. Constraints (6.11) prevent from straddling two pre-cross connected sub-structures. This set is very large, only a limited number of its constraints are added, other constraints are dynamically added when they are violated. Constraints (6.12) are integrality constraints.

In order to feed the master problem with p-structures found by the pricing problem, we need to express the parameters a_ℓ^s and b_ℓ^s as functions of the variables of the pricing problem: a_ℓ^s encodes the available number of backup paths for link ℓ, either ℓ is part of the pre-cross connected structure, which implies that $x_\ell^{\mathcal{BCK}} > 0$, or none of these two cases (i.e., is not protected by the pre-cross connected structure). Thus,

$$a_\ell^s = x_\ell^{\mathcal{BCK}} + \inf\left\{x_\ell^{\mathcal{T}}, 1 - x_\ell^{\mathcal{OXC}}, \lfloor 1 - \varepsilon x_\ell^{\mathcal{BCK}} \rfloor\right\}, \varepsilon << 1$$

Parameter b_ℓ^s encodes the spare capacity used by the p-etree on link ℓ. A spare capacity channel is used either by the basic tree (on-tree), or by the pre-cross connected part of the p-etree. Thus,

$$b_\ell^s = \sup\left\{x_\ell^{\mathcal{OXC}}, y_i^j + y_j^i\right\} \qquad \ell = \{i, j\} \in L$$

These two parameters a_ℓ and b_ℓ are used in the master problem as the protected capacity and the used protection capacity, respectively.

6.5 Performance Results

In this section, we compare the protection performance of the new p-etree protection approach to three other approaches: Pure p-tree scheme, and simple and non-simple p-cycle schemes presented in Chapter 5. We compare the four approaches based on their protection efficiency and flexibility and on their recovery delays.

6.5.1 Network Model

We consider four network topologies: NSF, COST239 - 19 links, New Jersey LATA, and COST239 - 26 links, each has an average nodal degree of 3, 3.4, 4.1 and 4.3, respectively. In order to investigate on how the link spare capacity budget affects the capacity efficiency, we selected three random distributions of link spare capacity budgets for each network topology. Each random distribution is characterized by its average spare capacity p on each link and its standard deviation σ. For the first distribution (first set of vertical bars in each sub figure in Figure 6.6), all the links of the network have been assigned the same transport capacity (60 channels) and the same spare capacity (20 channels), thus $(p, \sigma) = (20, 0)$. Other distributions are described in Figure 6.6 (x-axis).

6.5.2 Protection Efficiency

In Figure 6 6, we illustrate the variation of the number of protected capacity units (channels) as a function of the spare capacity budget distributions. The first observation is that, when all the links of any of the considered networks are allocated the same maximum spare capacity (first distribution), then the p-etrees and the non-simple p-cycles provide the same protected capacity. In such a case, the simple p-cycle protection provides $\sim$ 4%) less protected capacity, and the pure p-tree $\sim$ 50% in the first two networks (sparse networks) and $\sim$ 30% in the two last networks (more connected networks). The equivalent performance of the non-simple p-cycle and p-etree schemes tells us that the protection building blocks in the p-etree scheme are purely cyclical structures (non-simple p-cycles).

In the second and third distributions, we extended the link spare capacity budget to the interval $[0, 30]$, and performed a random selection of the spare capacity according to the illustrated distributions. The protected capacity provided by all the protection approaches is different from the case where a uniform spare capacity was applied. Within all the considered spare capacity budget distributions, the p-etree protection provides the highest amount of protected capacity units. The

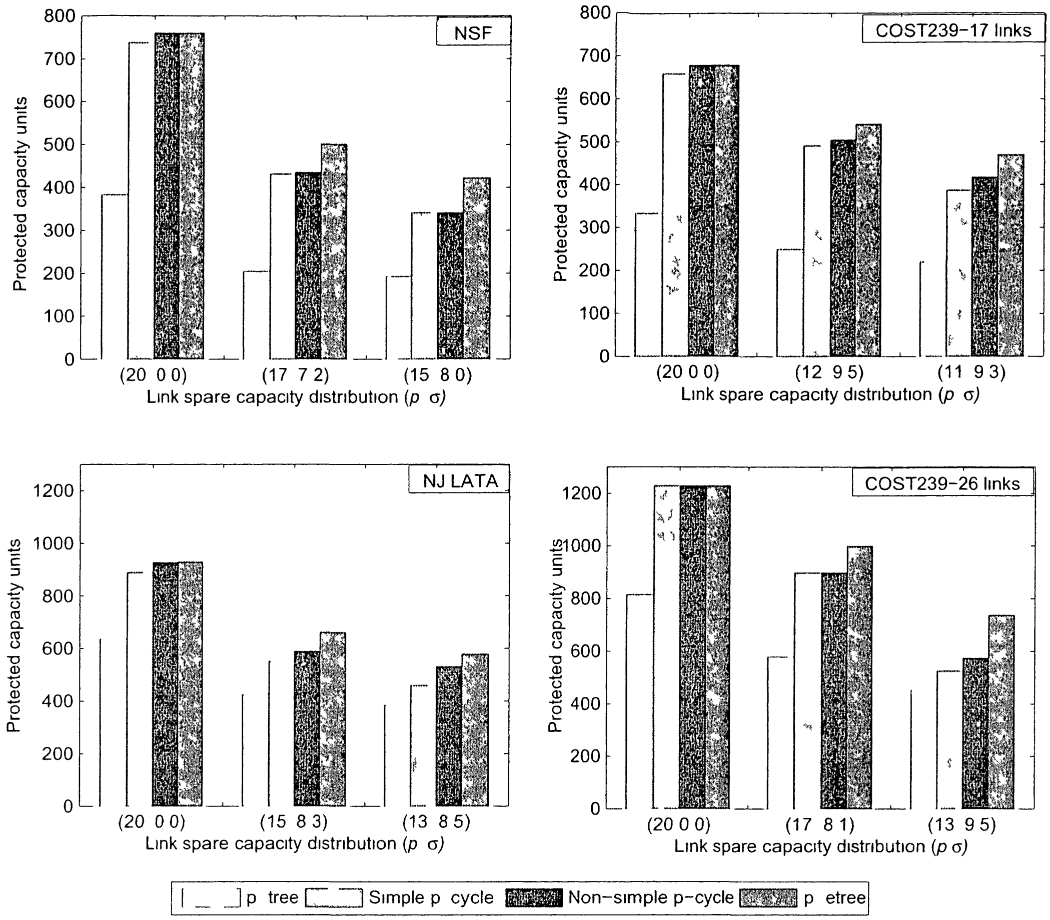


Figure 6 6 Distribution of the Protection Capacity

protected capacity by the p etree in the COST239 26 links is 23%, 28% and 43% better than that provided by the non simple p cycle simple p cycle, and p tree protection, respectively The amount of protected capacity decreases as the discrepancy σ of the link spare capacity distribution increases This is due mainly to the lack to flexibility of the cyclical protection structures

Table 6 1 illustrates the drop in the amount of protected capacity (%) due to the new distributions of spare capacity in COST239 26 and NJ LATA networks All four protection schemes are sensitive to the dispersion of the link spare capacity values (increase of σ) The p etree has the least drop among all four compared schemes The p tree is the second less affected scheme by the new distribution of spare capacity (distribution 2 in COST239 26 links and the NJ LATA network) The results in Table 6 1 give us a clear indication that linear patterns can be of higher flexibility over cyclical patterns, especially with the constrained spare capacity budgets.

The advantage of the p-etree protection over the p-cycle (either simple or non-simple) ones in terms of capacity efficiency is due to the protection building blocks in the p-etree-based protection scheme. Indeed, as pure cyclical, linear and hybrid structures are combined by the p-etree scheme, the resulting protection plan cannot be less efficient or less flexible than any of the pure cyclical or linear based protection schemes.

		p-tree	p-cycle		p-etree
			simple	non-simple	
COST239	Dist 1	29%	27%	27%	18%
	Dist 2	44%	57 %	53%	40%
NJ LATA	Dist 1	33%	37%	36%	28%
	Dist 2	39%	48 %	42%	32%

Table 6.1: Drop in Protected Capacity (%)

6.5.3 Recovery Delay

In order to evaluate the recovery delay of the p-etree-based protection scheme, we looked at the shape of its protection structures. Table 6.2 gives the recovery delay of the p-etree protection plan in the second distribution of link spare capacity (last set of bars of all sub figures in Figure 6.6). The results show that between $\sim$ 80% and 90% of the protection capacity is a pre-cross connected capacity. and 10% to 23% requires an additional delay of only $T+P$ to restore from any link failure. The percentage of protection capacity that requires a restoration delay ≥ 2 (T+P) is very low $\leq 2\%$. Thus. a high restoration delay compared to any totally pre-cross connected scheme is obtained. The distribution of the recovery delay over these three values, which are in turn associated with some p-etree structures, gives an insight on the shape of the p-etree protection structures

	$D + C$	$D + C + T + P$	$\geq D + C + 2(T + P)$
NSF	81%	17%	2%
COST239 -19 links	89%	11%	0%
NJ LATA	85%	15%	0%
COST239-26 links	77%	23%	0%

We assume $D_n = D, T_n = T$ for all n
and $P_\ell = P$ for all ℓ, to simplify the exposure.

Table 6.2: Recovery Delay Distribution

6.6 Conclusion

In this chapter, we proposed a novel pre-configured protection scheme where a priori no restriction is imposed on the shape of the protection building blocks. By extending trees, we built a pre-configured extended-tree (p-etree) protection scheme where the number of pre-cross connected backup paths are implicitly optimized by the explicit optimization of the protected working capacity. We compared our scheme to three other pre-configured schemes, and showed that it is more capacity efficient than all pure p-cycle and p-tree based schemes and still, achieves a recovery delay comparable to the delay of totally pre-cross connected schemes.

CHAPTER 7

The Pre-Configured Protection Structure Scheme

7.1 Introduction

In Chapter 5, we proposed new efficient design techniques of PWCE using fully pre-cross connected protection p-cycles (simple and non-simple) schemes. The protection building blocks in p-cycle schemes are pure cycles. Later on, in Chapter 6, we extended the p-cycle based approach, and proposed a novel protection approach based on hybrid protection structures that can be a priori of any shape. This approach, named *p-etree*, has the advantage that it includes a larger number of different shape protection structures than pure p-cycles. In p-etree based schemes, fully pre-cross connected structures are augmented with partially pre-cross connected structures by extending p-trees. Therein, the protection topologies are made of hybrid structures of trees and cycles (see Chapter 6 for typical structures). We showed the advantage of the p-etree approach in terms of flexibility, efficiency, and recovery time for different network scenarios, and that the protection structures tend to be more fully pre-cross connected when the link spare capacity budget is uniform, but partially within non uniform link spare capacity budget However, a question arises after these two chapters is: *How would the capacity efficiency vary if we consider all possible protection structures without any regard to their pre-cross connectivity , i.e., not only pure and hybrid structures.?*

Regarding the flexibility in provisioning protected capacity, the use of totally pre-cross connected structures like p-cycles, although it guarantees a low recovery delay, can be sometimes less flexible than dynamically cross connected schemes, e.g., in sparse networks [HS07], or with a constrained link spare capacity budget (see Chapters 5 and 6). From chapters 5 and 6, there is a clear trade-off between the pre-cross connectivity of protection schemes and their flexibility in provisioning protected capacity. We believe that a fully pre-cross connected scheme, even though it simplifies the recovery process in case of failure, has a price in terms of protection capacity and reliability.

Another issue in the design of PWCE that we have not much considered in the previous two chapters is the shaping of the PWCE. The shaping concern is to find the most appropriate PWCE, not necessarily the maximum size, that would minimize the blocking rate when dynamic traffic is carried in the network. This problem has been approached by a multi-objective ILP model in [She06]. In Chapters 5 and 6, we adopted a lower bound on the link protected capacity in order to shape the PWCE. However, finding the appropriate routing of the potential working capacity in the PWCE that will guarantee 100% protection for the upcoming dynamic traffic with the given link spare capacity budget is not an obvious activity.

In this chapter. we will further investigate the trade-off between the pre-cross connectivity and flexibility of protection schemes. and investigate shaping strategies of PWCE in order to maximize the end-to-end protected capacity. To achieve our objectives, we propose a new PWCE design approach based on pre-configured protection structures (p-structures) where pre-cross connectivity is not part of the objective (implicitly or explicitly). Rather, we favor the reliability and capacity efficiency of the resulting protection schemes For the end-to-end optimized PWCE. we use the p-structure concept, and propose an integrated protected and protection capacity optimization in order to maximize the protected capacity flow circulation in the network.

The rest of the chapter is organized as follows. In Section 7.2 we present our motivation and goals regarding the two design objectives targeted in this chapter We illustrate by an example the advantages of a p-structure based approach over the pure p-cycle and hybrid p-etree approaches. In Section 7 3 we present efficient ILP optimization models based on CG techniques for optimized hop-by-hop and end-to-end PWCEs. Next, in Section 7.4, we compare the performance of our new p-structure based PWCE design with the p-cycle based one. Conclusions are drawn in Section 7.5.

7.2 Motivation and Goals

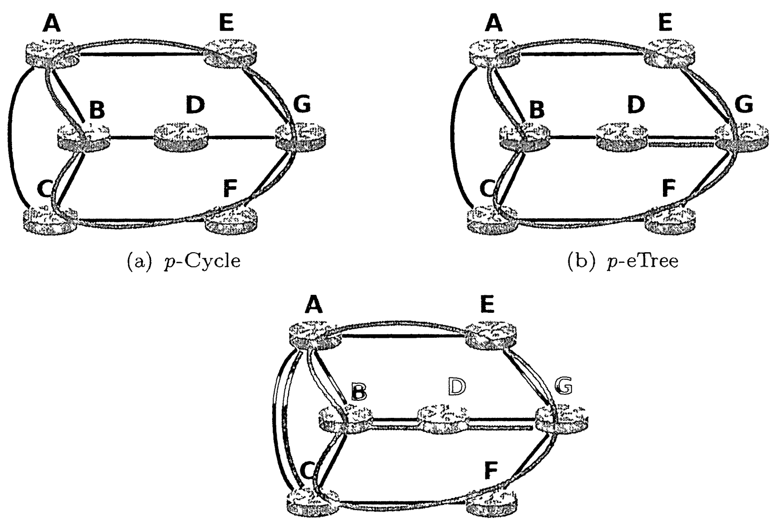
Based on the results in Chapters 5 and 6, we clearly see the advantage of using hybrid shape protection structures in order to offset some disadvantages of some pure shape protection structures. The construction approach of protection structures in the p-etree method focuses on some specific hybrid shape structures (see Figure 7.1). Although, a variety of shapes are considered as potential patterns, there are still further shapes to explore and investigate in order to improve different quality-of-service (QoS) parameters related to protection.

7.2.1 The p-Structure Concept

By p-structures we mean all possible protection structures in the network, i.e., no restriction is applied in the design process, and no pre-defined shape structure is used as an initial pattern as in the p-etree based approach. By doing so, we aim at selecting the most valued protection structures that will effectively provide the protection level in the network independently of their shapes. Though, no need to select p-cycles in order to meet the ring-like recovery delay, or any other shape protection in order to optimize any other protection parameter. In this approach of design of survivable WDM optical networks, by using p-structures, QoS parameters related to protection will be optimized independently of the shape of the protection structures. *It is the shapes of the protection structures that are adapted to meet the QoS parameters, not the shapes that define the protection performance of the protection scheme.* In other words *the design problem focuses on the protection parameters, not on which protection patterns can achieve those parameters* . In the next two sections, we present some advantages of using p-structures over p-cycles and p-etrees in the design of optimized PWCE.

7.2.2 Flexibility in Protection Capacity Allocation

In Figure 7.1, we illustrate three optimal protection models of PWCE based on p-cycles, p-etrees, and p-structures. We suppose a link spare capacity budget of one wavelength channel on each link. In the p-cycle and p-etree approaches, the link spare capacity budget is not fully used. Not because it is not needed, but because it is impossible to allocate any spare capacity following the pre-planned shape allocation plane, i.e., following p-cycles and p-etrees. Though, their lack of flexibility in using the spare capacity. The p-structure based scheme uses all spare capacity budget and spans all the links in the network. Regarding the requirement in terms of reconfiguration in order to recover from any link failure, the p-cycle scheme will not require any reconfiguration at intermediate nodes of any protected link; the p-etree scheme will require a reconfiguration at node G in case of a failure on link $B - D$; and the p-structure scheme will require the following reconfigurations at nodes a_i in case of a failure on link ℓ (a_i,ℓ): (B, $D - G$), (G, $B - D$), (G and C, $A - B$), (G and A, $B - C$).



(a) p-Cycle (b) p-eTree

(c) p-Structure

Figure 7.1: p-Structure vs. p-eTree vs. p-Cycle

Table 7.1 illustrates the distribution of the protected capacity in the three previously illustrated protection schemes. In the p-structure scheme, we use three and two more spare channels than the p-cycle and p-etree, but we provide four and three more protected channels than the p-cycle and p-etree schemes. respectively.

Links	p-cycle	p-tree	p-structure
{A,B}	1	1	**2**
{A,C}	2	2	2
{A,E}	1	1	1
{B,C}	1	1	**2**
{B,D}	0	1	1
{C,F}	1	1	1
{D,G}	0	0	**1**
{E,G}	1	1	1
{F,G}	1	1	1
Total	8	9	12

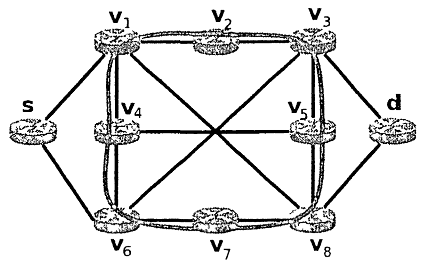
Table 7.1: Protected Capacity Distribution in p-Structure, p-eTree, and p-Cycle

7.2.3 Optimized End-to-End PWCE

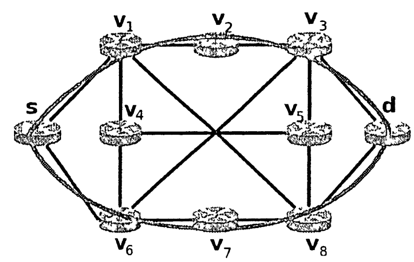
In this section, we focus on local optimal PWCE to minimize the blocking rate in dynamic provisioning based on PWCE. In Chapters 5 and 6, we focused on the designs that find the global optimal size of the PWCE by using some constraints that set a lower bound on the protected capacity budget (see Constraints 5.4). However, this approach does not necessarily guarantee a minimum blocking rate in the network, neither a maximum protected capacity flow circulation. In shaped PWCE, to be efficient, a PWCE design should be adapted to the distribution of the traffic over the node-pairs. Mathematically speaking, the shaping approach in Chapters 5 and 6 may cause difficulties to the optimization problem in finding feasible solutions, especially when a limited link capacity is assumed. Indeed, the lower bounds on the link protected capacity should be chosen with high care, otherwise the problem may not have a feasible solution.

In Figure 7.2, two designs of PWCE based on p-cycles are illustrated. We assume that each link has one unit of spare capacity budget. In Figure 7.2-(a), the proposed design is adapted to guarantee a maximum protected capacity flow circulation among nodes v_i, but not from/to s and d. The design in Figure 7.2-(b) offers another protected capacity flow circulation among other nodes. In this configuration, a communication between nodes s and d is guaranteed two backup paths in case of a failure, while less traffic among nodes v_i is provided protection in comparison to Figure 7.2-(a)

These two designs are based on p-cycles. In the next section, we propose optimization models



(a)



(b)

Figure 7.2: Optimized End-to-End PWCEs

and solution methods based on CG to carry the optimization process with p-structures as protection building blocks.

7.3 Optimized Design of p-Structure Based PWCE

In this chapter, we see the power of the CG modeling and solution method. Indeed, pre-enumeration of all possible protection structures in a network is impossible and an impractical exercise, even if the network size is relatively small. CG with its powerful modeling and solution-exploring approach make the solution method as scalable and efficient as the previous CG-based p-cycle and p-etree methods.

In the next two sections, we present two CG based optimization methods to optimize the number of protected links (hop-by-hop) and number of protected links along paths (end-to-end) in the design of PWCEs.

7.3.1 Hop-by-Hop Optimized Size PWCE Using p-Structures

The shape of the next protection structure is not known a priori, rather, it is decided by the pricing problem based also on the dual variables of the master problem.

Master Problem

The master optimization problem is identical to the p-etree one in Chapter 7.3 2. indeed all the parameters, constraints and the objective are identical. The difference is in the protection structure solution space $\mathcal{S}$, which is much larger in the p-structure scheme than in the p-cycle scheme.

Pricing Problem

The pricing problem corresponds to the problem of generating one promising protection structure that improves the value of the current LP solution of the RMP. It corresponds to the maximization problem of the reduced cost of the master problem subject to a set of protection p-structure constraints. Thus, it is identical to the one in Section 5.4.3.

Let us next define the following variables:

$$p_\ell^{\ell'} = \begin{cases} 1 & \text{if } \ell' \text{ provides protection for } \ell \text{ in the current } p\text{-structure} \\ 0 & \text{otherwise,} \end{cases}$$

$$x_\ell = \begin{cases} 1 & \text{if } \ell \text{ is spanned by the current } p\text{-structure} \\ 0 & \text{otherwise.} \end{cases}$$

$y_\ell \in \mathbb{Z}^+ =$ the number of disjoint alternative protection paths for link ℓ.

Re-expressing the objective in terms of these variables leads to:

$$\max \left(\sum_{\ell \in L} \theta_\ell^1 \overbrace{y_\ell}^{a_\ell} - \sum_{\ell \in L} \left(\theta_\ell^2 + \theta_\ell^3\right) \overbrace{x_\ell}^{b_\ell} \right).$$

The constraints of the pricing problem (generation of a protection structure) can be written:

$$p_\ell^{\ell'} \leq x_{\ell'} \qquad \ell, \ell' \in L \tag{7.1}$$

$$\sum_{\ell' \neq \ell \in \omega(N)} p_\ell^{\ell'} \geq y_\ell \qquad N \subset V, \ell \in \omega(N) \tag{7.2}$$

$$x_\ell, p_\ell^{\ell'} \in \{0,1\} \qquad \ell, \ell' \in L \tag{7.3}$$

$$y_\ell \in \mathbb{Z}^+ \qquad \ell \in L. \tag{7.4}$$

Constraints (7.1) say that, for a given pair of links ℓ ℓ', ℓ' can provide protection for ℓ if and only if it is (ℓ') part of the current p-structure (spanned by the p-structure). Constraints (7.2) set the number of disjoint backup paths for link ℓ to the minimum number of incident links to the minimum cut (min cut problem) separating the two end-nodes of the protected link. This problem is equivalent to the flow circulation problem in graph theory [AMO93]. Depending on the network topology, and using a combination of a BFS (Breadth First Search) and a DFS (depth First Search) algorithm, starting from one of the end-nodes of a protected link ℓ, it is possible to enumerate all the cuts separating the two end nodes of ℓ. In our case, for each protected link ℓ, only a limited number of cuts (when needed) are dynamically added like user cuts during the optimization process. Constraints (7.3) and (7.4) are integrality constraints.

7.3.2 End-to-End Optimized Size PWCE Using p-Structures

In this section, we develop an ILP model and use CG in order to design protection planes that maximize the availability of protected capacity on an end-to-end basis by using p-structures.

Master Problem

The objective is to maximize the number of protected end-to-end working paths denoted by $w_{v_o,v_d} \in \mathbb{Z}^+$ between each pair of origin - destination (v_o, v_d) nodes involved in communication. It is written as follows:

$$\max \sum_{v_o,v_d \in \mathcal{V}} w_{v_o,v_d}.$$

We define a first set of variables $w^{\ell}_{v_o,v_d} \in \mathbb{Z}^+$ to be the number of paths carried along ℓ between a node pair v_o. v_d. Furthermore, the two parameters $a^s_\ell \in \mathbb{Z}^+$ and $b^p_\ell \in \{0,1\}$ which encode the number of disjoint alternative protection paths for link ℓ and spare capacity utilization on link ℓ in the current p-structure p, respectively, and the link transport capacity (w^F_ℓ) and link spare capacity budget (ψ^F_ℓ) are kept unchanged from the model in Chapter 6.

Constraints of the master problem are written as follows:

$$\sum_{\ell \in \omega(N)} w^{\ell}_{v_o,v_d} = w_{v_o,v_d} \qquad N \subset \mathcal{V}, o \in N, d \notin N \tag{7.5}$$

$$\sum_{s \in S} a^s_\ell z^s - \sum_{v_o,v_d \in \mathcal{V}} w^{\ell}_{v_o,v_d} \geq 0 \qquad \ell \in \mathcal{L} \tag{7.6}$$

$$\sum_{s \in S} b^s_\ell z^s + \sum_{v_o,v_d \in \mathcal{V}} w^{\ell}_{v_o,v_d} \leq w^F_\ell \qquad \ell \in \mathcal{L} \tag{7.7}$$

$$\sum_{s \in S} b^s_\ell z^s \leq \psi^F_\ell \qquad \ell \in \mathcal{L} \tag{7.8}$$

$$w_{v_o,v_d} \geq w^{\min}_{v_o,v_d} \qquad v_o, v_d \in \mathcal{V} \tag{7.9}$$

$$w^{\ell}_{v_o,v_d}, z^s, w_{v_o,v_d} \in \mathbb{Z}^+ \qquad v_o, v_d \in \mathcal{V}, s \in S. \tag{7.10}$$

Constraints (7.5) are used to route flow through cuts separating node pairs v_o, v_d involved in a communication. These constraints are added dynamically only when they are needed as user cuts. Constraints (7.6) guarantee link protection for all working paths along each link ℓ carrying traffic between all node-pairs. Constraints (7.7) limit the overall working and protection capacity of a link ℓ to its transport capacity (w^F_ℓ). Constraints (7.8) set the link spare capacity budget. These two sets of constraints are similar to those in the previous master problem. Constraints (7.9) set a minimum working capacity between each node pair $\{v_o, v_d\}$ ($w^{\min}_{v_s,v_d}$ is a parameter). Constraints (7.10) define the domains of the optimization variables. Recall that the set S of p-structures grows dynamically as the pricing problem generates new p-structures that are added to the master problem.

Pricing Problem

As the new working flow variables are not directly considered in the definition of the reduced cost of the master problem, the pricing objective problem remains the same as in the previous model in Section 7.3.1

7.4 Performance Results

In this section we evaluate the new PWCE design approach based on p-structures, and compare its performance with the p-cycle based approach. The objectives of the p-cycle (simple and non-simple) schemes in Chapter 5 are to maximize the size of the PWCE on a hop-by-hop basis. Though, to be fair in the comparison process, we decided to compare the hop-by-hop p-structure based model to the non-simple p-cycle model in Chapter 5. Recall that the non-simple p-cycle set includes simple as well as non-simple p-cycles. In the remaining of this chapter, we refer to this set as p-cycle set.

As in Chapter 5, we define the reliability of a protection scheme as the ratio of protected capacity over the sum of protected and unprotected capacities. In addition to the reliability, we evaluate the capacity redundancy, and the average length of the backup protection paths in both the new p-structure based PWCE design and the p-cycle based one The backup path length is a significant parameter in the recovery process Indeed, longer restoration paths result in longer restoration delays and potential exposure to multiple optical impairments.

Performance evaluation and comparison are conducted on four networks: NSF, COST239, NJ-LATA, and USA all presented in Chapters 5 and 6. We assume a link spare capacity budget to be uniformly distributed in the interval (20%. 40%) of the transport capacity of each link.

The comparison of the capacity redundancy in Figure 7.3 shows that the design approach of PWCE using p-structures is less redundant than the one using pure p-cycles. For all four networks.

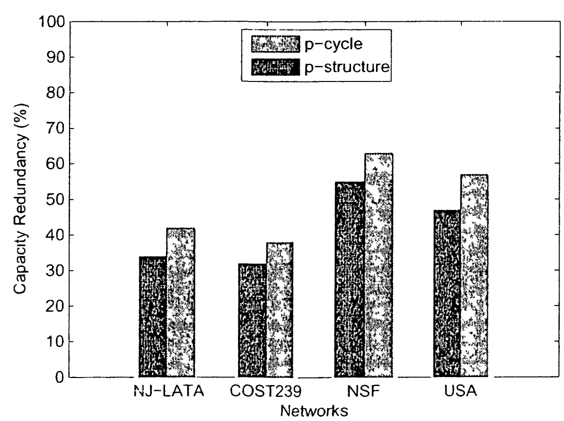


Figure 7.3: Capacity Redundancy: p-Structure vs. p-Cycle

the p-cycle based design approach is more capacity redundant (require more spare capacity) than the p-structure approach. We observe that the difference in capacity redundancy is higher ($\sim$ 10%) when the network topology is relatively sparse (NSF and USA networks).

In Figure (7.4), we compare the reliability (function of the PWCE size) of the two PWCE design approaches based on p-structures and p-cycles. We see that the new design approach using p-structures provides more protected capacity (higher reliability) than the one using only pure p-cycles in all four considered networks. With respect to reliability, the new design approach outperforms the pure p-cycle one by a ratio of up $\sim$ 15%. Combined with the previous results on capacity

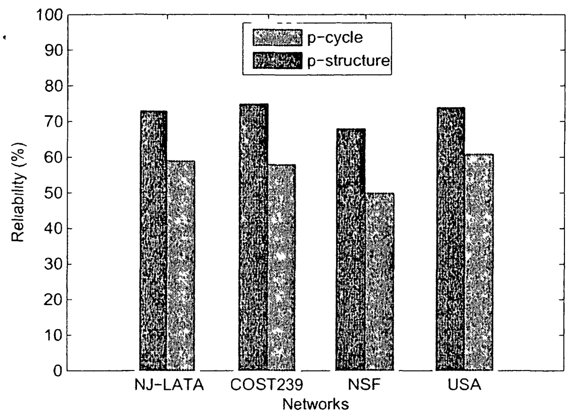


Figure 7.4: Reliability: p-Structure vs. p-Cycle

redundancy, we conclude that due to its flexibility in provisioning protection capacity, the PWCE using p-structures uses more efficiently the spare capacity, and provide larger PWCEs than the fully pre-cross connected p-cycle scheme. Herein, we use $\sim$ 10% less spare capacity, and provide $\sim$ 15% more protected capacity.

The average backup path length is directly related to the capacity redundancy of the protection scheme. In sparse networks where the network connectivity is low, there is less flexibility in setting up some pre-specified shape structures. e.g.. p-cycles that usually require a specific link spare capacity budget distribution to be efficient. Figure 7.5 gives the average length of the backup path in the p-structure and p-cycle based designs. The average backup path length in the p-cycle based design is larger than in the p-structure based one. It is well known that large p-cycles are more capacity efficient than small ones. However. due to its flexibility in provisioning protection capacity. the new

PWCE design approach using p-structures uses more efficiently the spare capacity (less redundant), provides larger PWCEs (more reliable), and guarantees shorter recovery paths compared to the p-cycle based design approach.

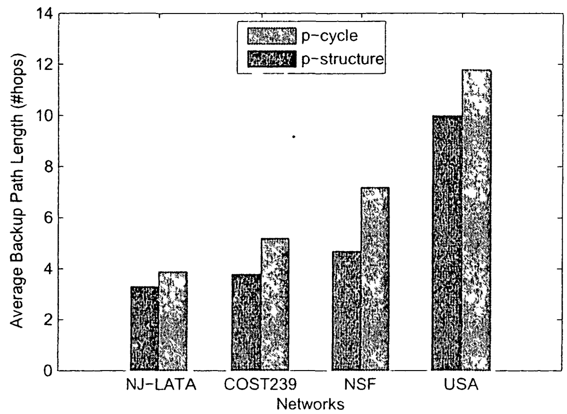


Figure 7.5: Average Backup Path Length· p-Structure vs. p-Cycle

7.5 Conclusion

We proposed a new way to design Protected Working Capacity Envelopes (PWCEs) in survivable WDM networks by using pre-configured protection structures with unrestricted shapes (arbitrary shape patterns) in order to maximize the protected working capacity in a hop-by-hop and end-to-end basis.

We showed the advantages of using p-structures over p-cycles in terms of flexibility and efficiency, especially within sparse networks and constrained link spare capacity budgets In order to cope with the large solution space of p-structures. we developed an ILP optimization model, and used CG decomposition method to scale the solution method. Results show that a design of PWCE using p-structure patterns is $\sim$ 10% less capacity redundant. $\sim$ 15% more reliable. and allow recovery along shorter backup paths compared to the p-cycle based scheme.

CHAPTER 8

Differentiated Quality-of-Recovery in Survivable WDM Mesh Networks

8.1 Introduction

The design problem of protection schemes in survivable WDM networks consists to find a trade-off among several parameters including capacity efficiency, recovery delay, management and operation complexity, and network availability time. In the previous Chapters 5 to 7, we considered the design problem of survivable WDM networks in the context of PWCE. We started with some pre-defined shape protection structures of pre-defined performances, i.e., p-cycles in Chapter 5, extended to pre-defined shape hybrid structures, i.e., p-etrees in Chapter 6, and ended up with non pre-defined shape structure (p-structures) in Chapter 7. This research direction is motivated by the search for more flexible protection structures to provide protection with different constrained spare capacity budgets and network models. The performances of protection schemes using pre-defined shape protection structures can be predicted because of the shape of the protection building blocks. For instance, p-cycles offer a good trad-off between recovery delay and capacity efficiency, but they are not scalable and not flexible; and p-trees offer high flexibility and scalability, but they are not capacity efficient. The advantage of using p-structures in the design of protection schemes is that the protection limits (e.g., flexibility) due to the shapes of the protection structures are overcome.

Furthermore, p-structure based schemes can be optimized to meet different protection parameters, e.g., recovery delay, protection capacity. Indeed, for a given targeted QoS protection parameter, using p-structures will result in a more flexible and efficient protection scheme. Because, among all protection structures in the networks, the ones that effectively guarantee the targeted QoS protection parameters will be chosen.

The fierce competition in the telecommunication world forces network operators to diversify their service portfolio in order to attract diverse customers with different telecommunication needs. In order to respond to the needs of as many customers as possible, the trends in current transport networks are evolving toward providing various services and applications with different bandwidth and service availability time requirements at different rates through the same network facility. Indeed, not all services require the same service availability time, neither all end-users are willing to pay high rates for the services they receive. Due to the multi-dimensional aspect of the design problem of protection schemes in survivable WDM networks, differentiation of QoR can be the solution method in order to strike a balance between the involved design parameters and cost for both service providers and customers.

In Section 3.2.2, we discussed the importance of recovery differentiation in the design of protection schemes in survivable WDM networks. In this chapter, we further investigate the design problem of protection schemes that guarantee different *recovery classes*, also referred in this chapter as differentiated Quality-of-Recovery (QoR).

In this chapter, we propose new design approaches of protection schemes based on p-structures, which optimize different protection parameters independently of the shapes of the protection structures, in order to achieve different classes of recovery. Our focus is on the design of protection schemes to explicitly optimize the recovery delay and the sharing of the protection capacity. Though, we develop a framework for QoR differentiation based on the pre-configuration of the basic protection structures. We propose three approaches of shared protection schemes to provide three classes of recovery based on pre-configured structures that are fully and partially (at some nodes) pre-cross connected ahead of failures, and dynamically reconfigured in case of failures.

This chapter is organized as follows. In Section 8.2, we present a quick review of the existing work in the literature on differentiation of QoS in survivable WDM networks. We give some motivation and goals of this chapter in Section 8.3. In Section 8.4, we present three design approaches of protection schemes, used in this study, in order to provide three equivalent QoR classes. We also provide some numerical comparison examples of the diversely pre-configured protection structures, and study the trade-off between the capacity efficiency and the recovery delay. In Section 8.5, we propose ILP models in order to optimize the quality-of-recovery of the strategies devised in Section 8.4, and adopt a CG modeling and solution method to solve them. Computational results are reported in Section 8.6.

8.2 Literature Review on QoS Differentiation in Survivable Optical Networks

Considerable research efforts have been made in recovery differentiation in survivable optical WDM networks [GS02, SGZ04, SM04, AKM03, BKLS01, DSST99]. Proposed differentiation strategies have focused on combining different quality of service protection parameters such as availability, reliability (quality of backup paths), and recovery delay.

The issue of providing differentiated QoS in terms of restoration delay versus capacity efficiency and management complexity in survivable all-optical networks has been studied in [BKLS01]. Therein, connections are classified into three categories according to their recovery delay requirements: Platinum (50 ms) for fastest recovery, gold (50-100 ms), and silver (1-10 s). In order to meet the recovery delay requirements, the authors used dedicated protection for connection in the platinum class, shared logical rings in the gold class, and a shared mesh scheme in the silver class. Although spare capacity saving is achieved with the gold and silver classes, the investment in platinum class to achieve the required recovery delay is at least 100% redundant, therefore, highly expensive.

In [AKM03], the authors proposed a Quality-of-Reliability (QoR) framework based on the recovery delay. The different classes of service are linked to a continuous linear function of recovery time in $[RT_{\min}, RT_{\infty}[$, where $RT_{\min}$ is the best possible recovery time, whereas RT_{∞} means no recovery is provided. Although the main factor is the delay, the authors neglected the queuing delay of control packets incurred at nodes where sequential signaling is performed, e.g., when switching nodes have to process many concurrent requests.

The problem of providing differentiated recovery delays in WDM is considered throughout the scheduling of control messages at the switching nodes in [SS04]. Control messages to set up different connections are processed according to their associated priorities. Though, a high priority request will be processed and its connection set up before any lower priority connection. An on-line scheduling heuristic, maximum-remaining-time-first (MRTF), to improve the worst case restoration time performance of each class has been proposed. In MRTF, the objective is to optimize the worst restoration time performance by giving priority to the tasks belonging to connections that are further away from completing the rerouting process.

In [DSST99], the authors considered different signaling strategies, and evaluated the recovery delay (i.e., OXC switching, transmission, and propagation delays) of three basic restoration methods based on their recovery signaling strategy in order to provide different recovery classes in survivable WDM networks. Different parameters were considered in the delay recovery including the propagation and processing delays of control messages and the number of cross connects at each switching node.

In the design of protection schemes in survivable WDM networks, there are different trade-offs between resource redundancy (cost), service unavailability time, recovery speed, traffic loss. and management overhead. We believe that, in order to efficiently provide a differentiated QoR, a better understanding of the recovery capabilities (protection and recovery time) of the protection building blocks is necessary. In the next section, we present our motivation and goals of the QoR classification based on the pre-configuration of the used protection schemes.

8.3 Motivation and Goals

The goal of this chapter is to develop design strategies of protection schemes in order to provide different classes of recovery throughout the best possible trade-offs among the different protection parameters. Our QoR differentiation strategy uses shared p-structures which are *diversely* pre-configured ahead of failures. Three classes of p-structures including fully pre-cross connected p-structures, partially pre-cross connected p-structures, and dynamically cross-connected p-structures are used. This classification is motivated by the trade-off, between the capacity efficiency and the recovery delay, each type of p-structures offers (see Section 3.6 for a simple comparison). In addition to the trade-off capacity efficiency - recovery delay, we emphasis in this chapter some others when combining several protection structures in global protection topologies.

In optical networks, either all-optical or opto-electrical, the recovery delay (i.e., from the time the failure appearance to the time the traffic is sent on the backup path) includes a failure detection delay, a cross connect switching delay, as well as control-message processing, queuing, and propagation delays (all together designated as the *recovery operation time* in Section 3.2.1). Failure detection delay is the time from the failure occurrence until the time the end nodes of the failing component start the recovery process. Cross connect switching delay is the time it takes to map (connect) an input port to an output port in a switch fabric along a backup path. Although, there are some differences among the various signaling protocols proposed in the literature to perform traffic recovery [DSST99, LYWK02, Ber03b], the recovery process generally involves sending a control message along the backup path and reconfiguring the optical cross-connects (OXCs) along the backup paths. The number of cross connects that need to be re-configured at a given node and along backup paths affect directly the end-to-end recovery delay of the underlying protection scheme. Indeed, control messages for cross connect re-configuration may need to be scheduled for processing after a queuing delay equal to the number of control messages waiting at each switching node. Though, the distribution of the number of cross connects that need a dynamic reconfiguration in case of a failure over the switching nodes is an important parameter in order to minimize the queuing and processing delays. This parameter is minimized in fully pre-cross connected schemes (only two end-nodes of an affected link) and differently optimized in partially pre-cross connected schemes.

8.4 Pre-Configured Protection: From Backup Reservation to Pre-Cross Connection

In shared capacity protection schemes, the shape of the basic building blocks has a major impact on the performance of the protection schemes. In this chapter, and in order to avoid any limitation inherent to the shape of the protection structures, we use protection structures of unrestricted shapes, i.e., all possible protection structures that can meet our design requirements and constraints. In Section 8.4.2 to 8.4.4 we discuss those different protection schemes together with their pros and cons.

8.4.1 Network Model and Signaling Strategies

Figure 8.1 illustrates the basic switching node model we will rely on in this chapter. We assume that the switching node supports separated signaling channels along different control channels, denoted by λ_{CTRL}, and that the channels passing through the switch fabric are exclusively dedicated to data.

The Optical Cross-connect (OXC), either transparent or opaque, is mainly composed of a switching fabric, and a set of input and output ports. The switching fabric is a re-configurable matrix of cross connects which is dynamically cross connected in order to map input ports to output ports to set up optical paths in the OXC switch. Pre-cross connected protection schemes can be planned with reconfigurable switch fabrics as well as with static non reconfigurable equipment (e.g., static ADMs) as they do not require any reconfiguration in case of a failure. The brain of the switch is its OXC processor. Indeed, it is responsible of resource management, and of coordinating the provisioning operations with other switching nodes. The control channels are electrically converted at each OXC processor, and next processed to decode the messages. The proposed OXC processor architecture is similar to the one in [Mae98].

The speed of the recovery process in case of a link failure depends on the number of cross connects that need dynamic cross connection at switching nodes involved in the recovery process. In fully

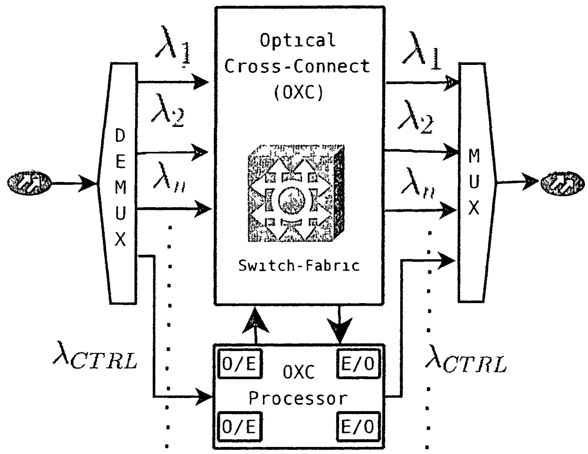


Figure 8.1: Switching Node Model

pre-cross connected backup paths, a dynamic switching is performed only at the two end-nodes of the failing link (path in case of path protection), with the traffic bypassing the intermediate nodes without any node reconfiguration. The cross connect switching delay is among the most time-consuming recovery operations in today OXC based switching nodes, it is estimated to be in the interval of 5-10 ms in MEMS based switches [DSST99]. The processing, propagation, and queuing delays of control messages come in addition to the cross connect switching delay that is incurred by a non pre-cross connected protection structure The processing delay is the time it takes for the message receiver to process a message and forward it to the message processor. The message processor manages queues where control messages waiting for processing, are queued. The signaling protocol in use to set up backup paths, can affect the queuing delay in the recovery process.

Our objective in this chapter is not to compare the performance of the signaling protocols regarding the recovery delay, rather, it is to design protection schemes that optimize the recovery delay independently of the signaling protocol in use. Next. we present three link protection schemes with different degrees of pre-cross connectivity of their protection structures, and discuss the trade-offs among their protection parameters.

8.4.2 Dynamically Cross Connected p-Structure Schemes

In this first approach, the protection relies on pre-calculated and reserved backup structures, but without cross-connection of input/output ports at the switch fabrics. Here, the focus is on extensive sharing of the spare capacity independently of its cross connectivity. Dynamic (on the fly) mapping of input and output ports through cross-connection at given OXCs are performed when protected links need protection capacity across some OXCs. Such a protection approach allows high flexibility in configuring the protection capacity, and efficient use of the protection capacity by multiple failure-independent (failure disjoint) working paths.

In Figure 8.2. we present an optimal design of a shared link protection scheme using an arbitrary shape protection structure (bold lines). The two working paths W_1 and W_2 (dashed lines) of one

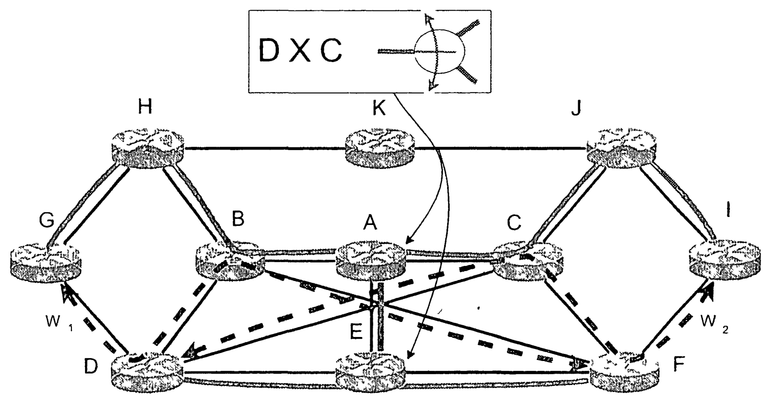


Figure 8 2: A Dynamically Cross Connected $p-$Structure Scheme

unit capacity (wavelength capacity) each, are protected by the shared protection structure (bold lines) of one unit backup capacity. The arrows starting at the box entitled "DXC" (for Dynamic cross-connection) and oriented to nodes A and E identify the cross connects that necessitate dynamic reconfiguration in case of any link failure in order to isolate any backup path. On the contrary, at the other nodes (except for A and E), there is a unique way to map each input port to an output port on the protection structure

Dynamic reconfiguration of cross connects allows end-to-end backup path isolation before traffic recovery. In Figure 8.2, a failure of any of the working channels will require a recovery signaling from the end-nodes of the failing link. and a dynamic cross connection at nodes A and E in order to set up (isolate) the inherent backup paths. In some OXC based technologies, dynamic reconfiguration of cross connects can seriously alter the recovery delay of such shared protection capacity schemes. In addition to the cross connection delay (switching delay), the queuing delay due to different failures on several channels may slow down the recovery process too. Indeed, when a node has to process several cross connection requests, a queuing delay of control messages - especially in sequential recovery signaling - is added to the recovery delay which increases the service unavailability time.

Table 8.1 reports the protection performance of the protection scheme depicted in Figure 8.2. Three parameters are presented: The capacity redundancy (CR), the average length of the backup paths, and the average number of cross connections that need to be dynamically reconfigured in order to isolate any backup path.

CR	Avg backup path length (# hops)	Avg # cross-connects
150%	3.66	2

Table 8.1: Protection Performance of a Dynamically Cross Connected $p-$Structure Scheme

Dynamic reconfiguration of the cross connects at node A and E allows flexible provisioning of the protection capacity, which in turn, results in short recovery paths (in average 3.66 hops). Although this scheme is more flexible and less expensive in terms of capacity redundancy, it suffers from the drawbacks of switching delay due to dynamic cross connection at some nodes of the backup paths.

8.4.3 Fully Pre-Cross Connected $p-$Structure Schemes

With a pre-cross connected protection scheme, in the event of a link failure, only the two end-nodes of the failing link need to perform dynamic switching of the traffic, with no additional reconfiguration at any intermediate node. Indeed, there is a unique way to map input ports to output ports in a totally pre-cross connected p-structure, thus no dynamic reconfiguration will be required in case of a failure. Local recovery can be performed with a limited signaling overhead if failure detection and recovery are implemented at the optical layer of the two end-nodes of the failing link. Therefore, with a fully pre-cross connected protection scheme, the recovery process is greatly simplified and management overhead is reduced as well as the service unavailability time. Examples of fully pre-cross connected protection structures are rings, pre-configured cycles (p-cycles) [GS98], and pre-cross connected trails (PXTs) [CCF04b].

In Figure 8.3, the two working paths are provided link protection by the illustrated shared p-cycle (bold lines). In case of a link failure, only the two end-nodes of the failing link will switch the working traffic from the failing working link onto the backup paths, intermediate nodes will *bypass* the traffic along the p-cycle without any reconfiguration.

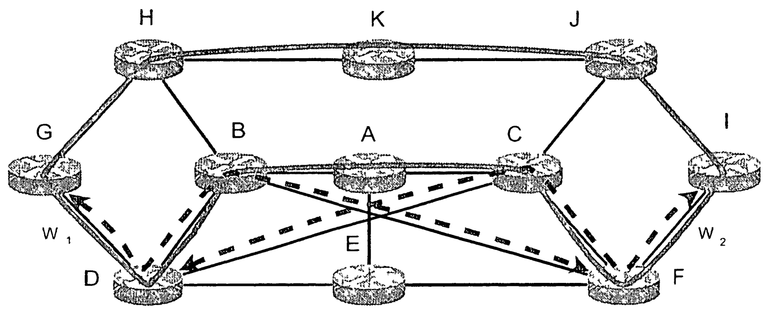


Figure 8.3: A Fully Pre-Cross Connected p-Cycle Scheme

Figure 8.4 illustrates a protection scheme based on shared PXTs which provides 100% protection to the proposed traffic model. The two PXT structures (bold lines) that define the protection scheme are shared and can be totally pre-cross connected ahead of any failure, and still provide 100% link protection without any reconfiguration in case of a failure.

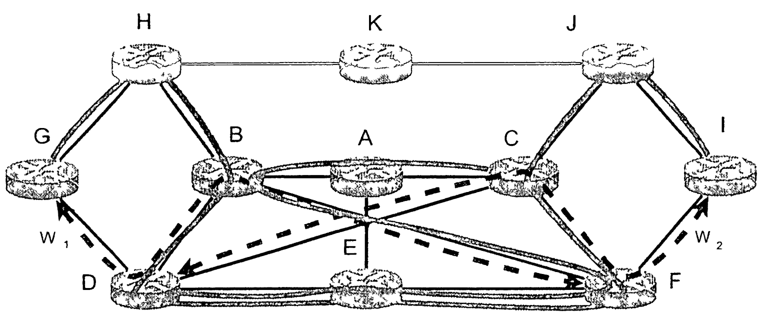


Figure 8.4: A Fully Pre-Cross Connected p-Trail Scheme

Table 8.2 illustrates the protection performance of the p-cycle and p-trail schemes in Figures 8.3 and 8.4, respectively. The capacity redundancy of the p-trail based scheme is higher than that of the p-cycle based one. However, the restoration path is in average 4 hops longer in the p-cycle scheme compared to the p-trail one. Thus, this may suggest that longer pre-cross connected structures are more efficient in terms of protection capacity, but result in longer restoration paths.

	CR	avg-bckp-path-length (# hops)
p-cycle	166%	7
p-trail	216%	3

Table 8.2: Performance Comparison: $p-$Cycle vs. $p-$Trail

However, these two shared p-structure are not the only ones that can be fully pre-cross connected ahead of failures and used without any reconfiguration in case of a failure. Figure 8 5 shows another p-structure which is not a p-cycle nor a classical p-trail, but still can be fully pre-cross connected and used without reconfiguration in case of a failure.

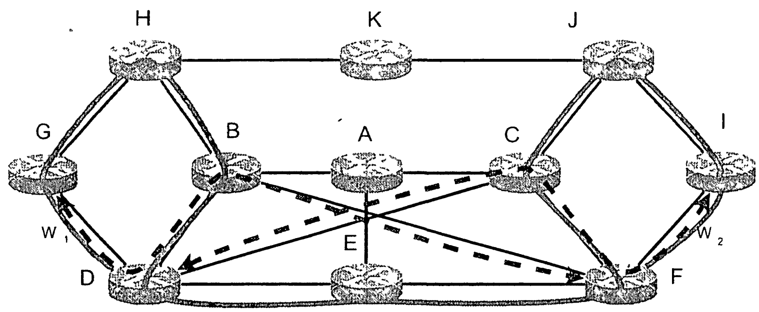


Figure 8.5: A Fully Pre-Cross Connected p-Structure Scheme

The reader may get confused when looking at nodes D and F, and say, there is more than one single way to map the three branches of the p-structure. However, at both nodes D (resp. F), the branches $\{B, D\}$ $\{D, E\}$ (resp. $\{C, F\}$ $\{E, F\}$) are by default mapped to recover from a failure on link $\{B, F\}$ (resp. $\{C, D\}$) and branch $\{D, G\}$ (resp. $\{F, I\}$) is ended locally at node D (resp. F). The only difference with the classical pre-cross connected structures is that the recovery process at a given node is performed through the already mapped protection branches, and there are no protection branches that are used locally to change the mapping of the protection capacity In Figure 8 5, in case of a failure on link $\{B. D\}$ (resp. $\{C. F\}$), the end-nodes B and D (resp. F and G) will switch locally on the two protection branches $\{D. G\}$ and $\{B, H\}$ (resp. $\{F. I\}$ and $\{C. J\}$). We define such a local switch reconfiguration as the *switching diversity* of fully pre-cross connected protection p-structure schemes.

Protection performance results of the fully pre-cross connected p-structure scheme in Figure 8.5 are given in Table 8.3. The fully pre-cross connected p-structure scheme gathers the capacity efficiency of the p-cycle scheme in Figure 8.3, and the average backup path length of the p-trail scheme in Figure 8.4. Indeed, it is capacity efficient as the p-cycle scheme and provides, in average, recovery along shorter paths as in the p-trail scheme.

CR	avg backup path length (# hops)
166%	3

Table 8.3: Protection Performance: Fully Pre-Cross Connected $p-$Structure

For the traffic distribution depicted in Figure 8.5, it is possible to find a p-structure that is totally pre-cross connected and capacity efficient at the same time. However, it is clear that dynamically reconfiguring the cross connects at some nodes provides more flexibility in setting up (isolating) backup paths. In the next sub section, we study a third protection approach that relies on partially pre-cross connecting some nodes, and dynamically reconfiguring other ones.

8.4.4 Partially Pre-Cross Connected $p-$Structure Schemes

In partially pre-cross connected protection schemes, we investigate how much the cross connectivity of protection structures does affect the trade-off between the capacity efficiency and the recovery delay. The reserved but dynamically cross connected protection capacity in dynamically reconfigured protection schemes allows high protection capacity sharing, but at the same time may suffer from some recovery inefficiency (larger delay, longer downtime, higher management overhead). On the other hand, fully pre-cross connected schemes guarantee low recovery delay, high availability, and less management overhead, but may result in more expensive protection cost. By partially pre-cross connecting the protection capacity, we aim at finding a good trade-off between these two protection capabilities.

Figure 8.6 shows a partially pre-cross connected p-structure which provides 100% protection against single link failures. In contrast with the protection scheme in Figure 8.2, this partially pre-cross connected p-structure scheme uses two protection channels on link $\{A, E\}$ which are mapped to the two branches $\{A, B\}$ and $\{A, C\}$ on the p-structure as illustrated.

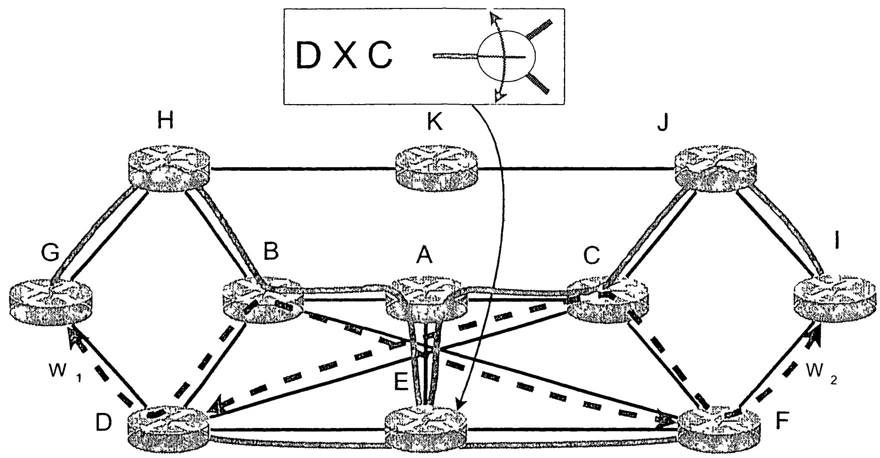


Figure 8.6: A Partially Pre-Cross Connected $p-$Structure Scheme

Table 8.4 illustrates the protection performance of the partially pre-cross connected p-structure protection scheme of Figure 8 6. Any failure on the working links will involve dynamic reconfiguration at the two end-nodes of the failing link and at node E Therefore, such a p-structure will require less signaling overhead and shorter switching delay in comparison to the p-structure scheme in Figure 8.2, but slightly higher spare capacity budget.

CR	avg backup path length (# hops)	# cross connects
166%	3 66	1

Table 8.4: Protection Performance: Partially cross connected $p-$structure

In Figure 8.6, the end-to-end cross connection delay is composed of one cross connect operation at intermediate node E in addition to those at the two end nodes of the failing link. In case where several copies of the partially pre-cross connected protection p-structure are required to provide protection to more working capacity, a queuing delay will be experienced by control messages at the OXC processor of node E, especially if sequential signaling and wavelength switching are used. In this case. and in order to limit the queuing delay and still guarantee a limited end-to-end switching delay, an equivalent p-structure where the reconfigurable cross-connect is moved from node E to A can be combined with the current one. In the resulting scheme. the reconfigurable cross connects will be divided between nodes E and A. Therefore. the protection scheme will simultaneously guarantee limited end-to-end switching and queuing delays at the reconfigurable switching nodes.

8.5 Optimized Designs of p-Structure Schemes

In this section, we propose optimization models based on CG in order to optimize the required spare capacity to provide 100% protection within the three proposed protection schemes presented in Section 8.4, i.e., dynamically cross connected, fully pre-cross connected, and partially pre-cross connected p-structure schemes. We propose the first optimized designs that explicitly limit the number of dynamic cross connects required at each switching node and along each backup path. The novelty in this study is that we do not restrict the shape of the protection structures to a specific shape (e.g., p-cycle, p-trees) in order to meet the specifications of any QoR requirement. Rather, all protection structures that can meet the QoR requirements are considered as candidate structures. Though, it is not the shapes of the protection structures that define the possible QoR, but the QoR requirements that define the shape of the protection structures.

In the next three subsections, we re-use the variables, parameters, constants, and sets of Chapters 5 and 7 in the definition of the optimization models of the previously defined protection schemes. We only introduce a new parameter $c_\ell \in \mathbb{R}^+$ for each $\ell \in \mathcal{L}$, which is the cost of using a wavelength channel on link ℓ, and change the variables $w^\ell_{v_o,v_d}$ into integer parameters by applying a shortest path routing algorithm in order to route the working traffic

8.5.1 Design of Dynamically Cross-Connected p-Structure Schemes

The focus in the dynamically cross-connected p-structure protection is on extensive sharing of the protection capacity (minimize the protection capacity budget) without worrying about the cross connectivity of the protection structures. Therefore, this approach is expected to be the most effective and flexible whatever the design constraints (spare capacity budget. traffic distribution, connectivity, ...).

Master Problem

We express the objective of the first master problem as follows:

$$\min \quad \sum_{s \in \mathcal{S}} \sum_{\ell \in \mathcal{L}} c_\ell \, b_\ell^s \, z^s \tag{8.1}$$

Subject to:

$$\sum_{s \in \mathcal{S}} a_\ell^s z^s \geq \sum_{v_o, v_d \in \mathcal{V}} w_{v_o, v_d}^\ell \qquad \ell \in \mathcal{L} \tag{8.2}$$

$$z^s \in \mathbb{Z}^+ \qquad s \in \mathcal{S} \tag{8.3}$$

The objective of this master problem is to minimize the spare capacity used by the candidate p-structures $s \in \mathcal{S}$ in order to provide 100% protection against single-link failures Constraints (8.2) reserve backup protection capacity for all working capacity in the network Constraints (8.3) define the domain of the optimization variables.

In order to cope with the size of the set of candidate p-structures, we adopt a CG modeling and solution method. Like in the previous CG optimization models, we develop a task oriented CG decomposition: The Restricted Master Problem (RMP) optimizes the selection of candidate p-structures, and the pricing problem generates new *augmenting* p-structures, i.e., p-structures that improve the value of the objective of the LP relaxation of the RMP.

Pricing Problem

The pricing problem corresponds to the minimization of the reduced cost associated to variables z^s in the RMP subject to a set of p-structure design constraints. The reduced cost is written as follows:

$$\min \quad \sum_{\ell \in \mathcal{L}} (b_\ell \, c_\ell - a_\ell \theta_\ell)$$

where θ_ℓ ($\ell \in \mathcal{L}$) are the dual variables associated with constraints (8.2) of the RMP.

Re-expressing the pricing objective in terms of these variables leads to:

$$\min \quad \sum_{\ell \in \mathcal{L}} \left(\overbrace{x_\ell}^{b_\ell} c_\ell - \overbrace{y_\ell}^{a_\ell} \theta_\ell \right).$$

The constraints of the pricing problem (generation of a single p-structure) at each iteration are written as follows:

$$p_\ell^{\ell'} \leq x_{\ell'} \qquad \ell, \ell'(\ell \neq \ell') \in \mathcal{L} \tag{8.4}$$

$$\sum_{\ell'(\ell' \neq \ell) \in \mathcal{E}(\mathcal{N})} p_\ell^{\ell'} \geq y_\ell \qquad \mathcal{N} \subset \mathcal{V}, \ell \in \mathcal{E}(\mathcal{N}) \tag{8.5}$$

$$\sum_{\ell'(\ell' \neq \ell) \in \mathcal{L}} p_\ell^{\ell'} \leq \alpha_\ell \, y_\ell \qquad \ell \in \mathcal{L} \tag{8.6}$$

$$\sum_{\ell' \in \mathcal{E}(v)} p_\ell^{\ell'} = 2\, n_v^\ell \qquad v \in \mathcal{V}, \ell \in \mathcal{L} \setminus \mathcal{E}(v) \tag{8.7}$$

$$x_\ell,\, p_\ell^{\ell'} \in \{0, 1\} \qquad \ell, \ell'(\ell \neq \ell') \in \mathcal{L} \tag{8.8}$$

$$n_v^\ell \in \mathbb{Z}^+ \qquad v \in \mathcal{V}, \ell \in \mathcal{L} \tag{8.9}$$

$$y_\ell \in \mathbb{Z}^+ \qquad \ell \in \mathcal{L} \tag{8.10}$$

where $\alpha_\ell \in \mathbb{Z}^+$ is an upper bound on the length of every backup path protecting link ℓ, and n_v^ℓ an integer variable used to protection capacity flow conservation at node v for each working link ℓ.

Constraints (8.4) and (8.5) are equivalent to Constraints (7.1) and (7.2) in Chapter 7. Constraints (8.4) set the protection relationship between links ℓ and ℓ'; and constraints (8.5) are flow conservation constraints to set the maximum protection capacity flow to the min cut separating the two end-nodes of a protected link ℓ (see [AMO93] for the maximum flow minimum cut problems). Constraints (8.6) are used to limit the average length of the backup paths used to protect working links. Constraints (8.7) are used to guarantee mapping of logical protection links at intermediate nodes of protected links (protection flow conservation constraints) Constraints (8.8), (8.9) and (8.10) are integrality constraints

8.5.2 Design of Fully Pre-Cross Connected p-Structure Schemes

In this section, we propose an optimization method to design protection schemes using p-structures that can be fully pre-cross connected ahead of failures. In order to extend the necessary conditions of pre-cross connectivity to protection structures that are not of pre-defined shapes like p-cycles and p-trails, we will use the following results.

Theorem 1. *At a given node v, if two incident links ℓ_1 and ℓ_2 are protecting a third link ℓ which is not incident at v, then, each of these two protecting links cannot be used alone in combination with a fourth link to protect another link, which is not incident to v.*

Proof. In order to prove the above results, we proceed by contradiction. We suppose that we can fully pre-cross connect a protection structure where at a given node v, there are three incident links ℓ_1. ℓ_2, and ℓ_3 in the protection topology, and that ℓ_1 and ℓ_2 provide protection for ℓ, and ℓ_1, or ℓ_2 can be combined with ℓ_3 in order to protect another link ℓ' which is not incident at v (see node 2 in Figure 8.7 for an example). Then, we end up with a contradiction. Indeed, in case a failure of ℓ or ℓ', a dynamic cross connection will be required at node v, thus the p-structure cannot be fully pre-cross connected ahead of failures. □

Figure 8.7 illustrates this protection condition. The working paths (W_i) are provided protection by the p-structure which spans all the network nodes (bold lines). The illustrated pre-configured protection structure can be pre-cross connected at node B as follows: Links {A,B} and {B,D} are mapped through node B, and link {B,C} is locally ended. By using the switching diversity based recovery introduced in Section 8.4.3, we can provide 100% for links {B,C} and {B.D} without any dynamic reconfiguration. In contrast to node B, node A requires dynamic reconfiguration in case of a failure of any of the two links $\{B, F\}$ or $\{E, G\}$. Indeed, by applying Theorem 1 at node A, links $\{A, B\}$ and $\{A. F\}$ are protecting working link $\{B. F\}$ (i.e., $p_{B-F}^{A-B} = p_{B-F}^{A-F} = 1$), but at the same time, link $\{A, F\}$ together with $\{A, E\}$ provide protection for link $\{E, G\}$. Therefore, the illustrated p-structure cannot be pre-cross connected at node A and provides protection for all the protected links without dynamic reconfiguration.

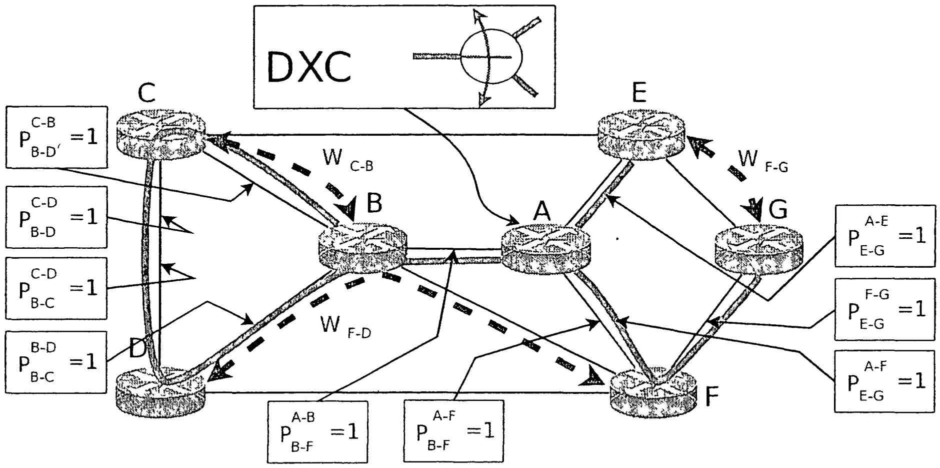


Figure 8.7: Requirements for Fully Pre-Cross Connected Capacity

Now, in order to avoid such a dynamic cross connection and still use all the possible p-structures in the network, we add the following variables and constraints:

- Variables

$$r_\ell^{v,\ell_1\ell_2} = \begin{cases} 1 & \text{if } \ell_1 \text{ and } \ell_2 \text{ incident at node } v \text{ protect link } \ell \\ 0 & \text{otherwise.} \end{cases}$$

- Constraints

Constraints (8.11) to (8.13) fix the above variables to their appropriate values in the pricing problem:

$$r_\ell^{v,\ell_1\ell_2} \geq p_\ell^{\ell_1} + p_\ell^{\ell_2} - 1 \qquad \ell \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell), \ell_1, \ell_2 \in \mathcal{E}(v) \tag{8.11}$$

$$r_\ell^{v,\ell_1\ell_2} \leq \min\{p_\ell^{\ell_1}, p_\ell^{\ell_2}\} \qquad \ell \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell), \ell_1, \ell_2 \in \mathcal{E}(v). \tag{8.12}$$

Constraints (8.11) fix the value of variables $r_\ell^{v,\ell_1\ell_2}$ to 1 if both ℓ_1 and ℓ_2 incident to v protect ℓ which is not incident to v. Constraints (8.12) set $r_\ell^{v,\ell_1\ell_2}$ to 0 if ℓ_1 or ℓ_2 does not protect ℓ.

$$r_{\ell}^{v,\ell_1\ell_2} + r_{\ell'}^{v,\ell_2\ell_3} - r_{\ell'}^{v,\ell_1\ell_2} \leq 1 \qquad \ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'), \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v) \tag{8.13}$$

$$r_{\ell}^{v,\ell_1\ell_3} + r_{\ell'}^{v,\ell_2\ell_3} - r_{\ell'}^{v,\ell_1\ell_3} \leq 1 \qquad \ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'), \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v) \tag{8.14}$$

$$r_{\ell}^{v,\ell_1\ell_2} + r_{\ell'}^{v,\ell_1\ell_3} - r_{\ell'}^{v,\ell_1\ell_2} \leq 1 \qquad \ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'), \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v). \tag{8.15}$$

Constraints (8.13) to (8.15) are used to avoid protection configurations like the one illustrated in Figure 8.7. Indeed, for any link pair ℓ, ℓ' and at any intermediate node v along the backup paths of both ℓ and ℓ', three protection-links incident at v cannot be shared for the protection of ℓ and ℓ', i.e., if ℓ_1 and ℓ_2 are protecting ℓ ($r_{\ell}^{v,\ell_1\ell_2} = 1$), and ℓ_2 and ℓ_3 are protecting ℓ' ($r_{\ell'}^{v,\ell_2\ell_3} = 1$) then unless ℓ_2 and ℓ_3 are protecting ℓ at the same time, this configuration is not allowed.

8.5.3 Design of Partially Pre-Cross Connected p-Structure Schemes

In this section, we propose a design approach that uses protection structures that can be partially pre-cross connected at some nodes. The focus is placed on mechanisms to explicitly optimize the number of cross connections that need dynamic reconfiguration in case of a link failure. Though, we minimize the number of dynamic cross connections at switching nodes in order to minimize the queuing delay, and the end-to-end reconfiguration delay along the backup paths. We design p-structures that individually guarantees limited end-to-end cross connection delay, and globally limited queuing delay at all switching nodes.

Master Problem

We extend the previous master problem by the addition of the following constraints:

$$\sum_{s \in \mathcal{S}} d_v^s z^s \leq \overline{n}_v^{\mathrm{OXC}} \qquad v \in \mathcal{V} \tag{8.16}$$

where variables $d_v^s \in \{0, 1\}$ for $s \in \mathcal{S}$ and $v \in \mathcal{V}$ equal to:

$$d_v^s = \begin{cases} 1 & \text{if } p\text{-structure } s \text{ requires dynamic cross connection at node } v \\ & \text{in order to recover from any link failure,} \\ 0 & otherwise; \end{cases}$$

and parameter $\overline{n}_v^{\text{OXC}}$ is an upper bound on the number of cross connects that need dynamic cross connection at node v in case of any link failure.

Constraints (8.16), which limit the number of dynamic cross connects at each node v, are intended to minimize the queuing delay that results from re-configuration of several cross connects at switching nodes.

Based on the new extended master problem, the objective function of the pricing problem becomes

$$\min \quad \sum_{\ell \in \mathcal{L}} \left(c_\ell \, b_\ell - \theta_\ell^1 \, a_\ell \right) + \sum_{v \in \mathcal{V}} \theta_v^2 \, d_v.$$

where θ_ℓ^1 and θ_v^2 are the dual variables associated with constraints (8.2) and (8.16), respectively.

Pricing Problem

In the pricing problem, we define the following new variables and constraints:

- Variables

$$t_v = \begin{cases} 1 & \text{if current } p\text{-structure } s \text{ requires dynamic cross connection at node } v \\ & \text{in order to recover from } \textit{any} \text{ link failure} \\ 0 & \text{otherwise,} \end{cases}$$

$$t_v^\ell = \begin{cases} 1 & \text{if a dynamic cross connection is required at node } v \text{ in order to recover from} \\ & \text{a failure on link } \ell \\ 0 & \text{otherwise.} \end{cases}$$

- Constraints

$$t_v^\ell \geq r_\ell^{v,\ell_1\ell_2} + r_{\ell'}^{v,\ell_2\ell_3} - r_{\ell'}^{v,\ell_1\ell_2} - 1$$

$$\ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'),\ \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v) \qquad (8.17)$$

$$t_v^\ell \geq r_\ell^{v,\ell_1\ell_2} + r_{\ell'}^{v,\ell_2\ell_3} - r_{\ell'}^{v,\ell_1\ell_2} - 1$$

$$\ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'),\ \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v) \qquad (8.18)$$

$$t_v^\ell \geq r_\ell^{v,\ell_1\ell_2} + r_{\ell'}^{v,\ell_2\ell_3} - r_{\ell'}^{v,\ell_1\ell_2} - 1$$

$$\ell, \ell' \in \mathcal{L}, v \in \mathcal{V} \setminus \mathcal{V}(\ell) \cup \mathcal{V}(\ell'),\ \ell_1, \ell_2, \ell_3 \in \mathcal{E}(v) \qquad (8.19)$$

$$t_v \geq t_v^\ell \qquad v \in \mathcal{V}, \ell \in \mathcal{L} \qquad (8.20)$$

$$\sum_{v \in \mathcal{V}} t_v^\ell \leq \bar{t}_\ell \qquad \ell \in \mathcal{L} \qquad (8.21)$$

  where $\bar{t}_\ell \in \mathbb{Z}^+$ is an upper bound parameter on the number of cross connects that need dynamic reconfiguration in order to recover from a failure on link ℓ

We re-use constraints (8.11) and (8.12) to set up the cross connect variables, and relax constraints (8.13), (8.14), and (8.15) in order to allow dynamic cross connections at some specific nodes. Constraints (8.17) to (8.19) are deduced from (8.13) to (8.15) by setting a variable t_v^ℓ to 1 when a dynamic cross connection is required in order to isolate a backup path of link ℓ. Constraints (8.20) are used to set up variables t_v when a dynamic cross connection is needed at node v in order to recover from any link failure. Setting a limit on the number of reconfigurable cross connects at switching nodes does not automatically solve the end-to-end recovery delay of connections. In order to remedy to this situation, constraints (8.21) impose a limit on the number of cross connects that need dynamic reconfiguration in order to set up an end-to-end backup path for any protected working link ℓ.

8.6 Computational results

In this section, we compare the performance of the three proposed protection schemes and the p-cycle in Chapter 5. Our objective is to optimize the required spare capacity to provide 100%

protection against single-link failures while meeting some design constraints in order to optimize different parameters of the recovery delay.

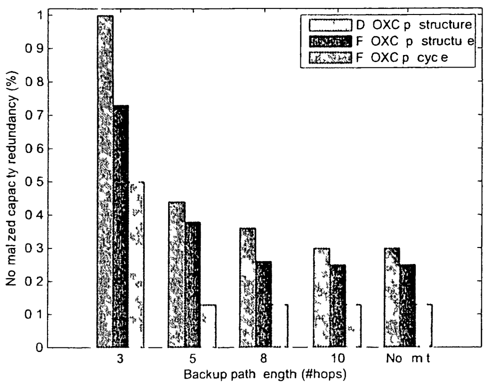
We use three network topologies characterized by a 3-uplet (number of nodes, number of links, average nodal degree): A (4×4) Manhattan (16, 24, 3), COST239 (11, 26, 4.72), and the NJ-LATA (11, 22, 4.1). These last two networks were presented in Chapter 5. We assume a uniform link cost model (c_ℓ) in the interval $[1, 10]$, and from now on, we refer to fully, partially, and dynamically pre-cross connected schemes by F-OXC, P-OXC, and D-OXC.

In the next three sub-sections, we focus on the trade-off capacity and reconfigurability of the protection schemes. First, we study how a maximum length bound on the backup paths affects the three protection schemes and the pure p-cycle one as studied in Chapter 5. Secondly, we focus on the trade-off between capacity efficiency and the number of reconfigurable cross connections in order to perform traffic recovery. Both the number of re-configurable cross connects at switching nodes and along backup paths are considered.

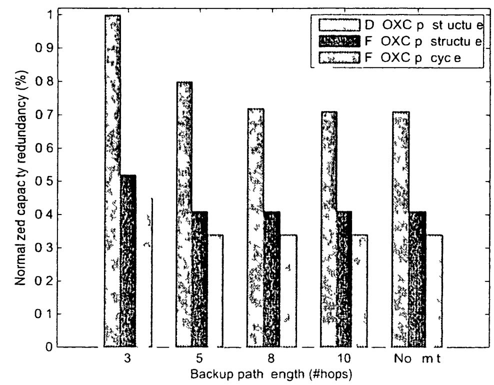
8.6.1 Backup Path Length vs. Capacity Redundancy

Figure 8.8 illustrates the variation of the normalized capacity redundancy as a function of the maximum backup path length expressed in terms of the number of hops. In this first set of experiments, we do not impose any restriction on the number of reconfigurable cross connects. Thus, the partially pre-cross connected (P-OXC) scheme is equivalent to the dynamically cross connected (D-OXC) scheme.

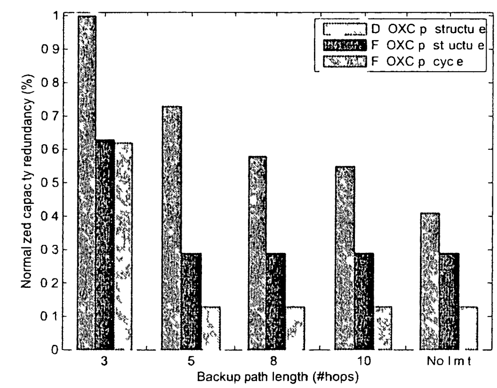
All compared schemes are sensitive to the maximum backup path length However, the most sensitive one is the fully pre-cross connected p-cycle (F-OXC p-cycle) scheme. The capacity redundancy of the pure p-cycle decreases as the length of the backup path bound increases, and it reaches its lowest bound when the maximum length of the backup paths lies in [8, 10] in COST239 and NJ-LATA, and greater than 10 in Manhattan 4×4. The fully pre-cross connected (F-OXC) p-structure scheme is less capacity redundant than the p-cycle, and reaches its lowest capacity redundancy bound earlier than the p-cycle scheme (in [5, 8]). Within the F-OXC p-structure scheme, all protection structures that can be fully pre cross connected ahead of failures, and used without any reconfiguration in case of a failure, are implicitly considered as candidate structures Thus, we preserve the pre cross connectivity of the protection scheme at a lower capacity redundancy in comparison to the F OXC p-cycle



(a) COST239 Network



(b) NJ LATA Network



(c) Manhattan (4×4) Network

Figure 8 8 Normalized Capacity Redundancy vs Maximum Backup Path Length

In Figure 8 8 we see that the difference in the capacity redundancy between the F OXC p cycle and p structure varies depending on the network connectivity The COST239 is relatively highly connected compared to NJ LATA and Manhattan 4×4 The F OXC p structure scheme is $\sim$ 10% less redundant than the p cycle based one, and in average $\sim$ 30% less capacity redundant in all the other network instances

When comparing the dynamically cross connected and the full pre cross connected p structure schemes, we see a difference of [10%, 20%] in their capacity redundancy due to the pre-cross connectivity of the F-OXC. In the D-OXC, a backup path shared by different link disjoint working paths, can be dynamically reconfigured at its intermediate nodes in order to isolate it. High sharing of the spare capacity (low redundancy) is achieved in D-OXC in comparison to the two F-OXC schemes. Moreover, because the D-OXC offers a high level of flexibility in setting up the backup paths, it reaches its capacity redundancy lowest bound earlier than the two other F-OXC methods. However, as no design constraints are considered to limit the number of reconfigurations at intermediate nodes along backup paths and at switching nodes, a switching and queuing delays will be generally added. It may prevent this scheme from scaling in large networks.

Next, we propose to study how much dynamic re-configuration is necessary to achieve the performance of the dynamically cross connected scheme from the fully pre-cross connected one. In order to close the gap between the capacity redundancy of these two protection schemes, we propose to use the partially pre-cross connected scheme. When no dynamic cross connection is accepted along any backup path, such a scheme becomes a fully pre-cross connected one, the other case where no constraint on the cross connects leads to the dynamically cross connected one. Next, we want to measure how reconfigurability should be added to the partially pre-cross connected scheme in order to achieve the same performance as the dynamically cross connected scheme.

8.6.2 End-to-End Dynamic Cross Connects vs. Capacity Redundancy

In Figure 8.9. we measure the capacity redundancy as a function of the maximum number of allowed dynamic cross connects along backup paths. The histogram illustrates the variation of the normalized capacity redundancy as a function of the number of allowed dynamic reconfigurations along each backup path. In this set of experiments, we do not limit the length of the backup paths. The first set of vertical bars corresponds to the fully pre-cross connected (F-OXC) p-structure scheme. In Figure 8.9. we see that as the maximum number of allowed dynamic cross connects increases, the capacity redundancy decreases to reach its lowest bound corresponding to the dynamically cross connected scheme (no limit on the number of dynamic cross connects). The most interesting part of the results in Figure 8.9 is how the capacity redundancy varies when the allowed number of dynamic cross connections along backup paths is bounded. Except for the Manhattan 4X4 topology where a maximum of 3 dynamic cross connections is required in order to achieve an optimal capacity redundancy, in the two other networks, only 2 are required. The capacity redundancy saving is in the range [15%, 35%] by allowing at most 1 dynamic cross connection along each backup path, and in the range [20%, 50%] with 2. In this case, the diameter of the network affects the capacity efficiency of the protection schemes. Both COST239 and NJ-LATA are 3-hop diameter networks, while the Manhattan is a 6-hop one. Therefore, as we do not limit the length of the backup paths, it is more likely that the Manhattan 4×4 will require more dynamic cross connections at intermediate nodes.

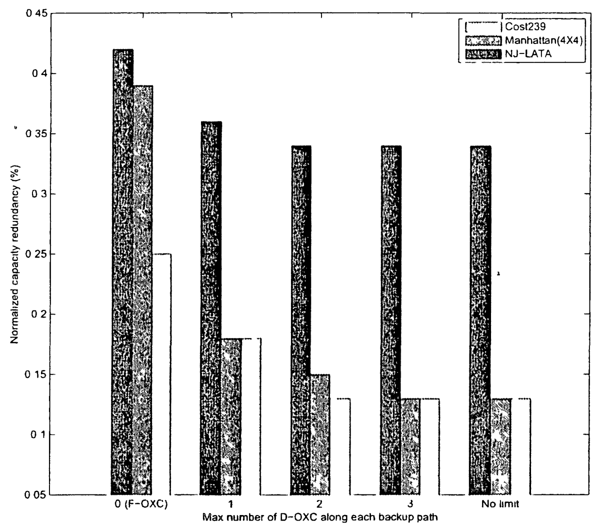


Figure 8.9: Normalized Capacity Redundancy as a Function of the Maximum Number of Reconfigurable Cross Connects Along a Backup Bath

Limiting the number of dynamic reconfigurations along each backup path is a solution to minimize the switching delay needed to isolate each backup path. However, when, at a given node, the number of needed reconfigurations to isolate a set of backup paths is high, a queuing delay of control messages will be added to the overall end-to-end recovery delay. In the next sub section, we propose to study how limiting the number of dynamic reconfigurations at switching nodes, in order to minimize the queuing delay, affects the capacity redundancy.

8.6.3 Number of Local Dynamic Cross Connects vs. Capacity Redundancy

In Figure 8.10, we measure the capacity redundancy of the partially pre-cross connected scheme as a function of the maximum number of allowed dynamic cross connects at switching nodes. The maximum number of dynamic cross connections required at each node in order to recovery from a link failure is evaluated by the size of the reconfigurable switching fabric. On the x-axis, we report on the maximum number of allowed dynamic cross connects at a given switching node as a percentage of the number of working paths going through that node. Though, 20% means that the size the reconfigurable switch fabric (or dynamic cross connects) reserved for protection is equal to 20% of the working path going through.

The fully pre-cross connected schemes can be envisioned with static switching fabrics where no dynamic reconfiguration is required in order to isolate the backup paths at intermediate nodes. As in Figure 8.9, we do not impose any bound neither on the length of the backup paths, nor on the number of reconfigurable cross connects along backup paths. Also, as in Figure 8.9, we consider the cases where no dynamic cross connections are allowed (first set of vertical bars corresponds to fully pre-cross connected schemes), and no limit on the number of dynamic cross connects (last set of vertical bars corresponds to dynamically cross connected scheme).

We observe the same trends as in Figure 8.9. However, the capacity redundancy reaches here its lowest bound when the maximum size of the reconfigurable switches used for protection is equal to number of working paths going through (100% of working paths). The saving in capacity redundancy is within a [10%, 35%] range. with reconfigurable switches of maximum size equal to 50% of the working paths, and tends to [15%, 55%] when the size is equal to 100%.

Results in Figure 8.10 are also useful in the dimensioning process of the switching nodes. The network resources can be shared between active working paths and their link disjoint protection counterparts, though reused in case of a failure on a working path. In such a case, and as with reconfigurable cross connects of size equal to the working paths going through them, it is possible to re-use not more than the end-nodes resources (e.g., transponders) used by working paths to provide

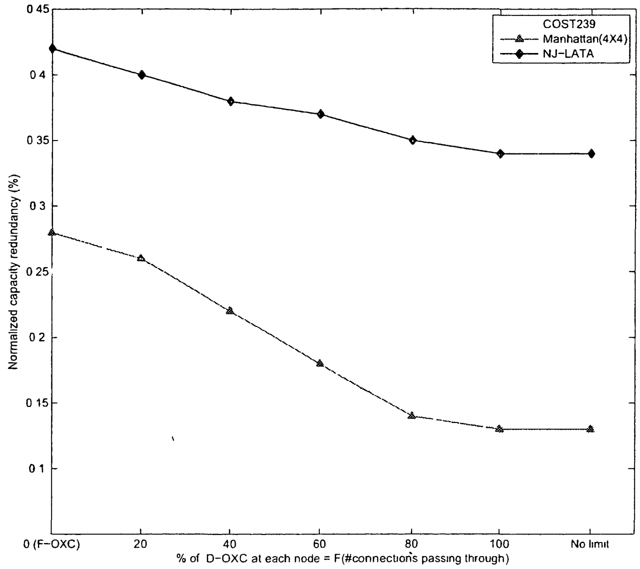


Figure 8.10: Normalized Capacity Redundancy as a Function of the Maximum Number of Reconfigurable Cross Connects at a Switching Node

protection without any additional cost.

8.7 Conclusion

Differentiation of quality of recovery is an important design technique in survivable WDM networks in order to strike a balance between the service availability and its cost. In this chapter, we proposed three optimized designs of protection schemes in survivable WDM networks to meet the requirement of three classes of recovery, and studied their requirements in terms of protection capacity.

We demonstrated that, in addition to the fully (end-to-end) pre-cross connected and the dynamically cross connected protection schemes. there is an efficient way to limit the dynamic reconfiguration of a protection scheme in case of a failure, and still provide high service availability at a low cost. By allowing only a limited number of cross connect reconfigurations along backup paths and at switching nodes, it is possible to save up to 50% of protection capacity and still provide an acceptable level of availability for different services.

To the best of our knowledge. this is the first study that has considered the three components of the recovery delay: the propagation, switching, and queuing delays, and proposed design methods to explicitly optimize each component separately and combinations of the different components. Depending on the used technology, the proposed protection schemes can be used to meet different quality of recovery and optimize any of the recovery delay components, or find a good trade-off between the different components.

CHAPTER 9

Differentiated Quality-of-Protection in Survivable WDM Mesh Networks

9.1 Introduction

Nowadays, the trends in the telecommunication business are moving toward multi-service platforms that will support different types of services and end-users, with different requirements and needs. In order to be competitive, a telecommunication business must be able to respond to the needs of as many customers as possible while minimizing its deployment and maintenance costs. Availability requirements in survivable transport networks depend on the type of customers using the network and the supported services. In today's telecommunication businesses. a variety of services with different protection guarantees, also called Quality-of-Protection (QoP), are proposed through the same network at different rates. In Chapter 7, we propose a framework for optimized design of differentiated QoR where different protection schemes with different spare capacity budgets provide different availability guarantees. In this chapter, we propose a framework to optimized designs of multiple QoP classes including single and dual-link failure scenarios in survivable WDM networks that use p-cycles and p-structures.

In modern telecommunication networks, some mission-critical applications. e.g.. tele-surgery.

require high network availability, e.g., 100%, which is not necessarily guaranteed by a 100% single-link failure protection scheme. In order to guarantee a high service availability, it takes recovery mechanism to protect against a large number of potential failure scenarios, e.g., dual-link and node failures. However, providing such a high network availability requires a protection capacity budget which is proportional to the targeted protection level. Differentiated QoP, which we refer to as the different guarantees of protection, can be the solution approach in order to optimize the network cost while providing different classes of protection. Indeed, not all the end-users and applications require the same level of resiliency against failures, some applications can perform even with a lower network availability than others, e.g., e-mail, and not all users can afford paying the cost of a guaranteed 100% service availability.

Different network availability analyses have been proposed in order to quantify the offered availability of different protection schemes [TN94, MCL$^+$03, HLS07]. However, most of those availability analyses have assumed that link failures in the network are independent from each other, and dual-link failures have not been considered much. The occurrence of dual-link failures, although less likely than single-link ones, is not unusual in modern optical networks [LDK01]. Resiliency against dual-link failures is the dominant factor in determining the service availability after a guaranteed resiliency against single-link failures.

Many factors may motivate the need of design methods to provide different protection classes including dual-link failures in resilient WDM networks. Single-link failure recovery schemes guarantee 100% recovery in case of a single-link failure within a short time (few milliseconds to few seconds depending on the protection scheme). However, the time it takes to repair the failing physical link may vary from a few hours to a few days. It may happen that a second failure occurs during the repair time of the first failure, thus leading to a dual-link failure during the same time period. Furthermore, telecommunication operators are facing the challenges of meeting *at least* the specifications of service-level agreements (SLAs) with their customers. Nowadays, some cooperative customers are asking in their SLA a service availability of 99.999% or higher [GR00a]. Therefore, it is of interest to understand and *measure* the provided availability in order to offer safer SLAs and competitive services, and though, avoid penalties. Another motivation for investigating dual-link failures is related to the SRLG concept (see Section 3.1.3). Indeed, failures on different optical fibers are not necessarily independent from each other for at least two reasons:

(1) Physical routing of optical links may differ from their logical routing counterparts, e.g., see Figure 3.1. The physical routing of links is dictated by different external constraints, e.g., sharing multi-purpose pipelines in cities, or minimizing design costs.

(2) Fibers are linked at switching nodes, and a partial (e.g., a port) or global node failure can easily cause a dual-link failure, e.g., see Figure 9.1. Such a case of figure is equivalent to a failure on a fiber-bypass at a given node, which, in case of a failure on one of its incident (at the node) links, make the other one unusable.

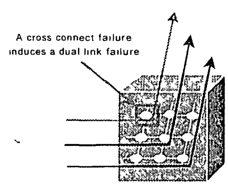


Figure 9.1: SRLG - Switching Node

Providing different classes of protection has been considered with single and dual-link failures. With single-link failures, Grover and Clouqueur proposed a multi QoP provisioning framework in survivable single-link failure networks [GC05]. Four protection classes were defined: guaranteed protection, best effort, unprotected, and preemptable services. The distribution of the multi-QoP services and their effect on the sharing of the protection capacity were studied. An ILP-based optimization model was proposed. In [TMP05], Tornatore *et al.* proposed a heuristic-based optimization approach within dedicated and shared path protection in order to achieve two different objectives: optimize the network availability, and minimize the number of fibers to provide the required QoP. However, the authors assumed in their availability analysis that optical nodes are perfectly reliable, and fiber links are mutually failure-independent.

The problem of dual-link failures has been studied within two failure scenarios: SRLG failures

[SYR05, SYR03, XXQL04], and arbitrary dual-link failures [HS03, CSC02]. In [HS03], He and Somani investigated the requirements in terms of protection capacity in order to provide an arbitrary double-link failure protection with the path and link based protection schemes. An ILP-based optimization method was proposed where three different backup paths between each source-destination node-pair were considered. With the optimization conditions, they showed that the path-based protection approach is more capacity efficient than the link-based one In [SZZW07], Shao *et al.* investigated the problem of providing differentiated QoP for surviving arbitrary double and single-link failures by allowing connections to choose among three different protection classes: Single Shared Path Protection (SSPP), Single Dedicated Path Protection (SDPP), and Double Shared Path Protection (DSPP). Routing algorithms were proposed, and the performance evaluation was focused on blocking probability and average QoP. In [CG05] Clouqueur and Grover proposed three ILP-based optimization models based on a pre-enumeration method of candidate protection paths in order to optimize the spare capacity required with multi-QoP services that can survive dual-link failures.

In this chapter, we are interested in optimal designs of protection schemes that use minimum spare capacity to provide different classes of QoP including 100% single-link failure protection ($R_1 = 100\%$) and different optimized dual-link failure protection (R_2). We investigate the design problem of protection topologies to provide the targeted QoP classes under arbitrary SRLG scenarios, and propose methods for optimizing the spare capacity within p-cycle and p-structure-based protection schemes.

This chapter is organized as follows. In Section 9 2, we give our motivation and goals Two issues are addressed in this section: the requirements in terms of capacity to provide single and dual-link failure protection, and the shape of the most resilient protection structures. In Section 9.3, we review some existing work on the design of protection schemes that can recover from single and dual-link failures. In Section 9.4, we illustrate, by using examples, the p-cycles capabilities in providing dual-link failure protection, and the advantage of using p-structures. In Section 9 5, we propose two different CG optimization approaches based on p-cycles and p-structures in order to optimize the required protection capacity in order to provide the targeted QoP classes. Section

9.6 is dedicated to computational results. We compute the required protection capacity in order to provide the targeted QoP classes, and establish a relation between the shapes of the protection structures and their protection efficiency. Section 9.7 concludes the chapter.

9.2 Motivation and Goals

The performance of any protection scheme in survivable WDM networks is mainly defined by the shapes of its protection building blocks. Different shared protection schemes, named after the shape of their protection structure, e.g., $p-$cycles [GS98], $p-$trees[XCT03, ZY02b], $p-$etrees in Chapter 6, and p-structures in Chapters 7 and 8, are either proposed or studied in this thesis in order to provide 100% protection against single-link failures. We conducted performance comparison studies to measure the efficiency of those pre-configured protection schemes with 100% single-link failure scenarios. However, some questions that have aroused our curiosity are:

- How would the protection efficiency of those schemes vary if they were to provide protection against different QoP classes including different R_2 levels?
- What are the shapes of the most efficient protection structures that can effectively guarantee at the same time 100% single-link failure protection ($R_1 = 100\%$) and different levels of dual-link failure protection (R_2).

In this chapter, and in order to answer these questions, we propose *quantitative* design approaches that guarantee different service availability levels including resiliency against 100% single-link failures and multiple dual-link failure scenarios.

We focus on the design process of p-cycle and p-structure based protection schemes in order to effectively extend their protection capabilities to support the different targeted QoP classes. In the p-cycle-based approach, as no exact optimization method exists, our goal is to develop efficient and scalable optimization tools in order to optimize the required protection capacity to provide the different targeted QoP classes. The p-cycles of the optimal solutions will be studied in order to establish a relation between their shapes and the provided QoP classes. In the p-structure-based approach, and by using all possible protection structures, our goal is to select the most efficient structures that can effectively meet the different QoP requirements. By doing so, we aim at giving a clear answer to the question about the shapes of the most efficient protection structures.

9.3 Literature Review on Design of Dual-Link Failure Protection Schemes

The literature on design of protection schemes to provide different QoP classes including dual-link failures is not rich. The p-cycle and p-tree are the two types of predefined shape protection structures that have been considered in the design of multi-QoP schemes in the literature [TT05, SGC04a, RC08, Sch03b, Sch03a].

Dual-link restorability in mesh networks protected by p-cycles was studied in [Sch03b, Sch03a, SGC04a]. In [Sch03b], Schupké et *al.* used directed p-cycles in the design of 100% single-link failure recovery schemes, and studied the trade-off between the number of p-cycles and the average dual-link failure restorability. Therein, the authors proposed an ILP model based on a set of candidate p-cycles that are enumerated ahead of the optimization process, and pre-configured to protect against some pre-defined dual-link failures. Even though the ILP model was solved to optimality, the best potential solution with such a two-step optimization approach can be far from the optimal one, see Chapter 5. In [SGC04a], different pre-selection strategies of p-cycles were proposed in order to reduce the susceptibility of p-cycles to some specific dual-link failures. p-Cycles with a lower susceptibility are selected as potential protection structures. Failure dispersal is another strategy for selecting p-cycles in order to spread the link protection over different p-cycles [SGC04a]. However, restricting the p-cycle selection affects the optimal design and the required number of p-cycles, as well as their length (see Chapter 5).

The design of p-trees to provide different QoP classes including dual-link failure in survivable WDM networks has been considered in [TT05, MFB99. XCT03]. In [TT05], Tang et *al.* proposed an

ILP model to minimize the spare capacity budget in order to provide 100% protection against single-link failures and a distributed provisioning algorithm for double-link failure restoration. Simulation results show that through dynamic re-provisioning around 70% of the double-link failures can be restored by the restoration scheme even though the spare capacity in the network is planned to stand against single-link failures.

In [MFB99], Médard et *al.* presented a design approach to construct a pair of directed spanning trees in a way that a failure of any single edge or node (except the root node) in the network, leaves all the nodes connected with the root node using at least one of the trees. They named their approach the red/blue trees. In [XCT03], Xue et *al.* extended the red/blue trees design, and included Quality-of-Protection (QoP) and Quality-of-Service (QoS). The QoP of a pair of red/blue trees was defined as the maximum number of simultaneous link failures that can be survived in the network. Heuristic algorithms were proposed for constructing a pair of red/blue trees with enhanced QoP, low total cost, and maximum bottleneck bandwidth.

In the previous Chapters 5 to 8, we have seen how restricting the shape of the potential protection structures can be harmful to the capacity efficiency of a protection scheme. In the literature, and to the best of our knowledge, the problem consisting to describe the shapes of the most resilient protection structures to dual-link failures has never been studied.

9.4 Dual-Link Failure Recovery: p-Cycle and p-Structure Based Protection Schemes

In this section, we present some illustrative examples of the protection capabilities of p-cycles and p-structures in providing different QoP classes associated to different R_2 levels.

9.4.1 Dual-Link Failure Recovery Based on p-Cycles

In this section, we investigate dual-link failure recovery without p-cycles reconfiguration. or rerouting. Unlike in [Sch03b], we consider bidirectional p-cycles. thus every straddling-cycle link has two backup protection paths. We focus on pre-configured static p-cycles which, in case of a failure, reroute the affected traffic without any dynamic reconfiguration of the spare capacity. In our study, a dual-link failure may affect any two links in an arbitrary order, in which case the affected traffic is switched onto the backup p-cycles in a way that guarantee the recovery of a maximum working capacity (see below the examples illustrated in Figure 9.3-(a) and Figure 9.4-(b)).

A 100% single-link failure protection scheme based on p-cycles can survive a dual-link failure provided that the failure happened on disjoint p-cycles (p-cycles that are not sharing any common link). We next discuss the cases when the affected links are protected by the same p-cycle, and analyze their impact on the network availability. In Figures 9.2 to 9.5, the dashed lines represent a one unit capacity p-cycle indexed from now on by s, and the numbers (1/2 means 1, or 2 units) on the links indicate the number of protected capacity units by the illustrated p-cycle.

Figure 9.2-(a) illustrates a case of a dual-link failure occurring on two links $A - B$ and $E - F$, which are on-cycle links and provided one unit of protected capacity by the current p-cycle s. In this case of dual-link failure. the protected capacity units will not be restorable on both links, i.e., not fully restorable working capacity. However, if s provides protection for only one of the links (e.g., see Figure 9.2-(b), protected capacity by s on link $E - F = 0$), the same dual-link failure scenario, even though not fully restorable, will only affect the capacity on the protected link ($A - B$).

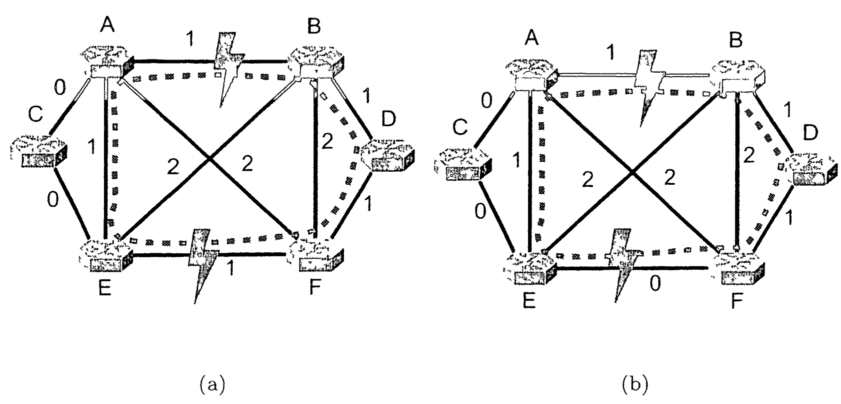


Figure 9.2: Dual-Link Failure Protection - Two On-Cycle Links

In Figure 9.3, we illustrate a dual-link failure scenario where one of the affected links is an on-cycle one and the second is a straddling-cycle one. In Figure 9.3-(a). we assume both links are protected by the illustrated $p-cycle$ s. Therein, the restorable capacity is at most 1 unit (independently of the order in which the failures have occurred, at most one working capacity can be restored). In Figure 9.3-(b), the on-cycle link $A - B$ belongs to s, but it is not protected by s (0 protected capacity). A dual-link failure on $A - B$ and $A - F$ will induce the same recovery process. However, in this case, the lost capacity, if any, is less than before.

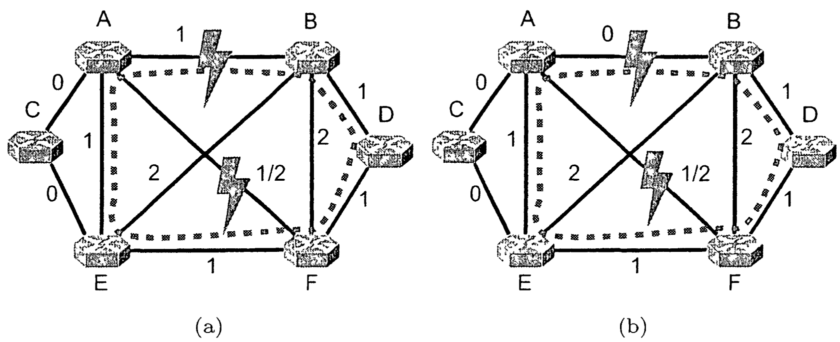


Figure 9.3: Dual-Link Failure Protection - On-Cycle/Straddling-Cycle Links

Figures 9.4-(a) and (b) illustrate two cases where the two failing links are provided protection by the illustrated p-cycles as straddling-cycle links. We can distinguish different configurations:

(i) Only the first failing link can be restored in case of a dual-link failure: Whether the two straddling-cycle links are guaranteed one or two protected capacity units, and independently of the order in which the failures have occurred, it is possible to reconstruct one or two alternate backup paths to recover the first affected link, but not the second one. In Figure 9.4-(a), a first failure on link $A-F$ followed by a second on $B-E$ will result in the following restoration scheme: switch the affected traffic on $A-F$ onto the backup path(s) $A-E-F$ $(A-B-D-F)$, and drop the traffic on $B-E$ (no backup capacity is left).

(ii) Working capacity from the two affected links can be fully or partially restored: this is only possible when the first failing link has less than two protected capacity units. Figure 9.4-(b) illustrates two failing links that are sharing the illustrated p-cycle. Suppose that $A - F$ had failed before link $B - F$, and that the protected working capacity on $A - F$ is one unit and

restored through $A - E - F$. Because it is possible to construct a second disjoint backup path $B - D - F$ on the same p-cycle, surviving a second failure on $B - F$ becomes possible. However, to be fully restorable, the two links should not have more than one protected capacity unit.

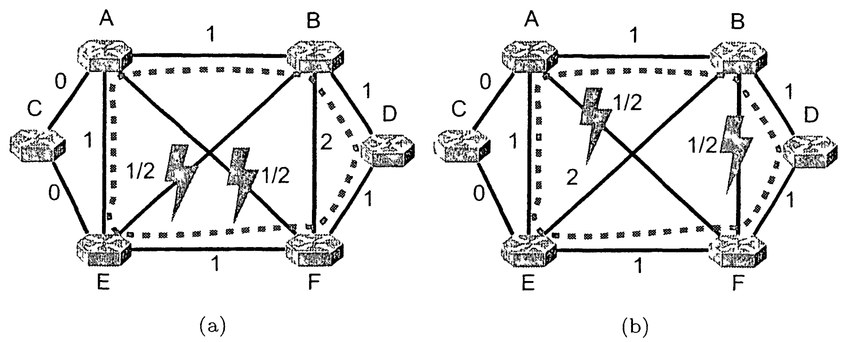


Figure 9.4: Dual-Link Failure Protection - Two Straddling-Cycle Links

A dual-link failure cannot be fully recovered if, from one end-node of a failing link, it is not possible to join its second end-node without crossing one of the two endpoints of the second failing link. A second example is illustrated in Figure 9.5. Even though the protected capacity is only one unit on links $C - D$ and $E - B$, the proposed p-cycle cannot survive a dual-link failure on those two links.

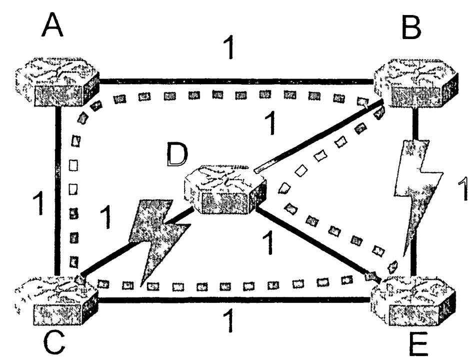


Figure 9.5: Dual-Link Failure Protection - Non Fully Restorable Configuration

In the next section, we illustrate by an example the advantage in terms of capacity efficiency and flexibility of using p-structures in the design of dual-link failure resilient protection schemes

9.4.2 Dual-Link Failure Recovery: p-Cycles vs. p-Structures

In Figure 9.6 is illustrated a network topology with its potential dual-link failures. The link pairs, which are susceptible to fail at the same time, are grouped in distinct SRLGs (e.g., $SRLG_1$ contains links $A-B$ and $A-C$ which are susceptible to fail at the same time). We assume a working traffic model where each physical link is carrying a wavelength connection.

- $SRLG_1 : A-B, A-C$
- $SRLG_2 : A-B, C-D$
- $SRLG_3 : A-B, A-E$
- $SRLG_4 : C-D, D-E$
- $SRLG_5 : C-D, B-D$
- $SRLG_6 : A-E, B-E$
- $SRLG_7 : B-E, C-E$

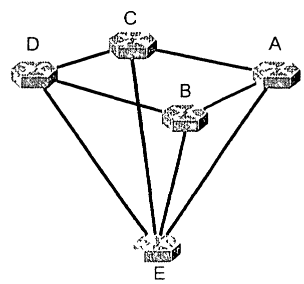


Figure 9.6: Arbitrary SRLGs.

In Figure 9.7, we illustrate the optimal combination of p-cycles that minimizes the required protection capacity in order to provide 100% protection against all single-link failures and the dual-link failures in Figure 9.6. The illustrated four p-cycles (bold lines) provide protection to the eight working links (dashed lines). We see that, except for the first p-cycle in Figure 9.7-(a) which is used at its full protection capacity (protect all its on-cycle links), all the three others are used at $\sim$ 38% (3/8) and $\sim$ 34% (1/3) of their total protection capacity. Indeed, no link-pair of the spanned links by the first p-cycle belongs to one of the SRLGs in Figure 9.6. However, to protect links that belong to the same SRLG in Figure 9.6, it takes more protection capacity to provide 100% protection (e.g., see the other three sub-figures). In this case, the shared p-cycles tend to be dedicated protection structures. The only way to protect a pair of links that belongs to an SRLG is to protect them as non intersecting straddling-cycle links, e.g., Figure 9.7-(d) (see Section 9 4.1). The p-cycle based scheme in Figure 9.7 provides 100% protection against all single-link failures and protection for only $7/\binom{8}{2} \times 100\%$ (7 link pairs out of $\binom{8}{2}$ pairs) of all possible dual-link failures. The cost of this optimal p-cycle protection scheme is 16 channels, thus its capacity redundancy is 16/8

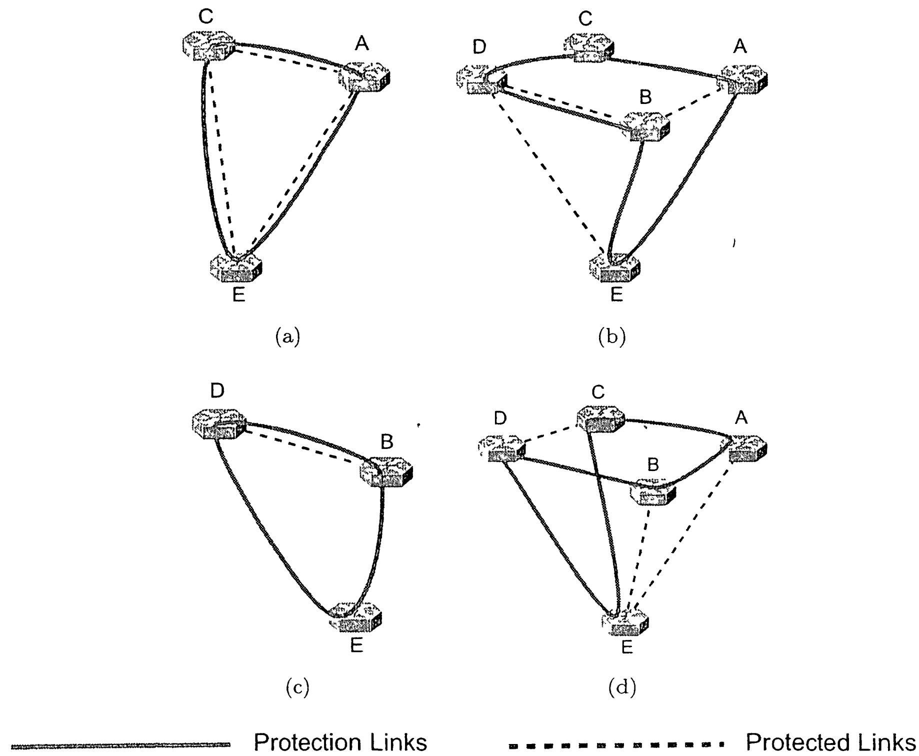


Figure 9.7: Dual-Link Failure Protection: A p-Cycle Based Protection Scheme

= 200%.

In Figure 9.8, we illustrate another optimal design of a protection scheme based on p-structures in order to provide protection within the previous network and failure models illustrated in Figure 9.6. The illustrated two p-structures provide 100% protection against all single and potential dual-link failures in the network. Compared to the previous p-cycle scheme in Figure 9.7 which requires 16 backup channels, the p-structure scheme illustrated in Figure 9.8 requires only 12 backup channels. Thus, it is more capacity effective than the p-cycle based scheme. Regarding the shapes of the protection structures in the p-structure scheme, the protection topologies are more connected, though, offer more routing possibilities in case of any single or dual-link failures. The problem of single and dual-link failure protection can be assimilated to the design of protection schemes with a constrained link spare capacity budget. Indeed, the constraint related to spare capacity distribution in the latter affect the flexibility of the protection scheme as well as the distribution of the link over SRLGs in the network.

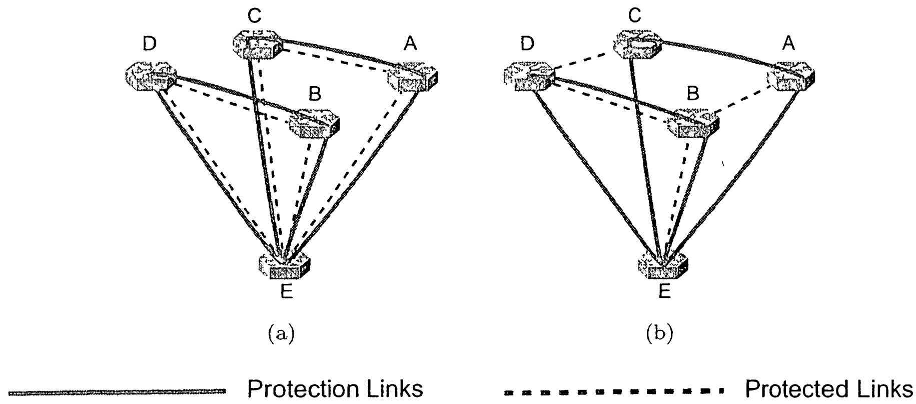


Figure 9.8: Dual-Link Failure Protection: A p-Structure Based Protection Scheme

9.5 Mathematical Optimization Models

In this section, we propose ILP-based optimization models to optimize the spare capacity needed to provide the targeted QoP classes, i.e., 100% protection against single-link failures and different protection classes against dual-link failures. Our optimization approach is based on CG where the definition of the shape and of the protection capability of each protection structure are integrated in the optimization process. Unlike the models in [Sch03b, SGC04a], the protection matrix of the p-cycles and p-structures are built and defines dynamically during the optimization processes. Indeed, following the CG approach, we iteratively construct the protection matrix until we reach the optimal value with respect to the design objective.

9.5.1 Network Failure Model

We propose optimization models where we are given a discrete probability distribution $P = (p_{\ell,\ell'})$ which associates a value in $\{0,1\}$ to each pair of links ℓ and ℓ' depending on whether they are susceptible to fail at the same time ($p_{\ell,\ell'} = 1$) or not ($p_{\ell,\ell'} = 0$) (or, belong to the same SRLG). Furthermore, and unlike the optimization models in [Sch03b] and [SGC04a] where one has to find appropriate weights for the components of a multi-objective optimization function, we propose to use the following R_2 formula based on the dual-link failure probability distribution.

$$R_2 = \frac{\sum\limits_{\ell,\ell' \in \mathcal{L}} p_{\ell,\ell'}}{\binom{|\mathcal{L}|}{2}}. \tag{9.1}$$

Formula (9.1) gives the number of link-pairs that are susceptible to fail at he same time over the total number of link-pairs.

9.5.2 Optimized Design of p-Cycle Based Protection Schemes

As in the previous CG models in this thesis, the optimization model for p-cycles design is divided into two sub-problems: the master and pricing problems. In this case, the master problem optimizes the selection of protection structures generated by the pricing problem, and the pricing problem dynamically generates p-cycles that can effectively provide the targeted QoP classes.

Master Problem

We assume that the working capacity w_ℓ on each link ℓ (routing of working paths) is given, and we re-use some of the variables, sets, and parameters defined in Chapters 5 to 8. In addition to the parameter a_ℓ^s and b_ℓ^s already defined in Chapter 5, for each p-cycle $s \in \mathcal{S}$ we define the following parameter:

- $d_{\ell\ell'}^s$ encodes the protection relationship between p-cycle s and links ℓ, ℓ'. It is equal to the number of protected channels that cannot be recovered in case of a dual-link failure on both ℓ and ℓ'.

The objective of the master problem is written as follows:

$$\min \left(\sum_{s \in \mathcal{S}} \sum_{\ell \in \mathcal{L}} b_\ell^s z^s \right).$$

The constraints of the master problem are as follows:

$$\sum_{s \in \mathcal{S}} a_\ell^s z^s \geq w_\ell \qquad \ell \in \mathcal{L} \tag{9.2}$$

$$\sum_{s \in \mathcal{S}} p_{\ell,\ell'} d_{\ell,\ell'}^s z^s = 0 \qquad \ell, \ell' \in \mathcal{L}. \tag{9.3}$$

Constraints (9.2) guarantee protection against all single-link failures for w_ℓ working channels on each link ℓ (100% single-link failure recovery). Constraints (9.3) guarantee 100% protection against all potential dual-link failures on all link-pairs ℓ, ℓ'. p-Cycles that do not protect against potential dual-link failures are forbidden in the optimal solution by this last set of constraints.

Pricing Problem

The pricing problem consists to minimize the reduced cost of the master problem subject to the p-cycle shaping and protection constraints. We define the variables of the pricing problem as follows:

$$x_\ell^o = \begin{cases} 1 & \text{if } \ell \text{ is an on-cycle link} \\ 0 & \text{otherwise,} \end{cases}$$

$$x_\ell^t = \begin{cases} 1 & \text{if } \ell \text{ is a straddling-cycle link} \\ 0 & \text{otherwise.} \end{cases}$$

The objective function of the pricing problem, i.e., the minimization function of the reduced cost associated to the variables of the master problem is written as follows:

$$\min \left(\sum_{\ell \in \mathcal{L}} b_\ell - \sum_{\ell \in \mathcal{L}} \theta_\ell^1 a_\ell + \sum_{\ell, \ell' \in L} \theta_{\ell\ \ell'}^2\, p_{\ell,\ell'}\, d_{\ell\ \ell'} \right).$$

where θ_ℓ^1. and $\theta_{\ell,\ell'}^2$ are the dual variable vectors associated with constraints (9.2) and (9.3), respectively.

The p-cycle shaping constraints are written as follows:

$$\sum_{\ell \in \omega(v)} x^o_\ell \leq 2 \qquad v \in \mathcal{V} \tag{9.4}$$

$$\sum_{\ell' \in \omega(v)\ \ell' \neq \ell} x^o_{\ell'} \geq x^o_\ell \qquad v \in \mathcal{V}, \ell \in \mathcal{V}(v) \tag{9.5}$$

$$2x^t_\ell \leq \sum_{\ell' \in \mathcal{V}(v)} x^o_{\ell'} \qquad \ell \in \mathcal{L}, v \in \mathcal{V}(\ell) \tag{9.6}$$

$$\sum_{\ell \in \mathcal{E}(N)} x^o_\ell \geq x^t_{\ell'} \qquad N \subset \mathcal{V}, \ell' \in \mathcal{E}(N). \tag{9.7}$$

Constraints (9.4) and (9.5) are used to shape the current p-cycle. According to these two sets of constraints, a p-cycle can have either 2 or 0 incident links at any given node $v \in \mathcal{V}$. Constraints (9.6) are used to set up straddling-cycle links. Constraints (9.7) are sub-cycle elimination constraints, and they are only added when needed using the so-called user cuts feature [ILO03].

Now that the current p-cycle is shaped, let us introduce additional variables in order to calculate the dual-link failure protection matrix. We need to distinguish two situations for a given link: *(i)* belonging to a p-cycle (whether on-cycle or straddling-cycle) and *(ii)* being protected by a p-cycle. For this reason, we define the following variables:

- $y^o_\ell = 1$, if ℓ is provided protection as an on-cycle link, 0 otherwise,
- $y^t_\ell \in \{0, 1, 2\}$, for a straddling-cycle link ℓ, this variable counts the number of protection paths for ℓ.
- $t_{\ell\ell'} \in \{0, 1, 2\}$, which encodes the vulnerability of the current p-cycle to a dual-link failure on links ℓ and ℓ'. $t_{\ell\ell'} = 0$ if the current p-cycle can fully survive a dual-link failure on links ℓ and ℓ', and $n \geq 1$ to count the number of lost link channels due to a dual-link failure on ℓ and ℓ'.

The next two sets of constraints (9.8) and (9.9) express the protection relationship between the current p-cycle and a link ℓ. Constraints (9.8) express that the current p-cycle can provide protection for its on-cycle links. Constraints (9.9) count the number of provided backup paths for a straddling-cycle link ℓ. Recall that in such a case, a link can be either on-cycle or straddling-cycle, but it is not necessarily provided protection (see the examples in Figures 9.2, 9.3, and 9.4)

$$y_\ell^o \leq x_\ell^o \qquad \ell \in \mathcal{L} \tag{9.8}$$

$$y_\ell^t \leq 2x_\ell^t \qquad \ell \in \mathcal{L}. \tag{9.9}$$

Let us now see how to measure the impact of a dual-link failure on a recovery scheme based on a single p-cycle s. In this section, we re-use the dual-link protection analysis presented in Figures 9.2, 9.3 and 9.4. We include the probability of a dual-link failure to occur in order to help the pricing problem in finding the globally most resilient p-cycles.

- If two links ℓ, ℓ' are on-cycle, and the current p-cycle provides protection for both of them ($y_\ell^o = 1, y_{\ell'}^o = 1$), then, the current p-cycle cannot fully survive a dual-link failure on these two links, see Figure (9.2)-(a). Constraints (9.10) set the variables $t_{\ell,\ell'}$ to the number of channels that cannot be recovered in case of a dual-link failure on ℓ and ℓ', and 0 otherwise. (the current p-cycle can fully survive a dual-link failure on ℓ and ℓ').

$$t_{\ell,\ell'} \geq 2p_{\ell,\ell'}(y_\ell^o + y_{\ell'}^o - 1) \qquad \ell, \ell' \in \mathcal{L}. \tag{9.10}$$

- If two links are on-cycle, and the current p-cycle provides protection for only one of them, e.g., $y_\ell^o = 1$ and $y_{\ell'}^o = 0$ (see Figure (9.2)-(b)), again, the current p-cycle cannot fully survive a dual-link failure on those two links, and constraints (9.11) set the variables $t_{\ell,\ell'}$ to their appropriate values (lower than the previous case).

$$t_{\ell,\ell'} \geq p_{\ell,\ell'}(y_\ell^o + x_{\ell'}^o - 1) \qquad \ell. \ell' \in \mathcal{L} \tag{9.11}$$

- Given ℓ and ℓ'. if one of the links is provided protection as an on-cycle link ($y_\ell^o = 1$) while the other link as a straddling-cycle (either one unit or two) ($y_{\ell'}^t = 1$ or 2). then, by (9 12). the current p-cycle cannot fully survive a dual-link failure on those two links, and $t_{\ell,\ell'}$ is set to the induced vulnerability, (see Figure (9.3)-(a)).

$$t_{\ell,\ell'} \geq p_{\ell,\ell'}(2y^o_\ell + y^t_{\ell'} - 2) \qquad \ell, \ell' \in \mathcal{L}. \tag{9.12}$$

- Given ℓ and ℓ', a similar case when one link, ℓ, is only used as an on-cycle link ($x^o_\ell = 1$) while the other link, ℓ', is provided protection as a straddling-cycle (either one unit or two) ($y^t_{\ell'} = 1$ or 2), then, by (9.13), the current p-cycle cannot fully survive a dual-link failure on those two links and $t_{\ell,\ell'}$ is set to the induced vulnerability, see Figure (9.3)-(b).

$$t_{\ell,\ell'} \geq p_{\ell,\ell'}(x^o_\ell + y^s_{\ell'} - 2) \qquad \ell, \ell' \in \mathcal{L} \tag{9.13}$$

The remaining cases to be looked at are when both links are protected while being considered as straddling-cycle links, see Figure 9 4-(a) and (b). The p-cycle in Figure 9.4-(a) cannot fully survive a dual-link failure on links $A - F$ and $B - E$, even when these two links are only transporting one unit of working capacity (other cases, e.g., two units on a given link and one or two units on the second one cannot be recovered). In Figure (9.4)-(b), due to the disjointness of backup restoration paths. it is possible to fully recover from a dual-link failure when the two affected links are transporting one capacity unit.

In order to distinguish the cases of Figures 9.4-(a) and 9.4-(b), we propose to use the following idea: remove one of the two affected links and all its adjacent links, and try to construct a second p-cycle that spans the remaining affected link. In order to put our idea in practice. we propose to use the following new variables $r^\ell_{\ell',\ell''}$ to encode whether there exists a protection path that spans ℓ when one of the links ℓ' or ℓ'' and its incident links are unusable (removed). Hence. $r^\ell_{\ell',\ell''}= 1$. when. after removing ℓ' and its incident links, there remains a backup protection path for ℓ'', 0 otherwise The following constraints are used to encode the vulnerability of a p-cycle to dual-link failures in such cases.

$$r^{\ell}_{\ell',\ell''} \leq x^{o}_{\ell} \qquad \ell, \ell', \ell''(\ell \neq \ell'') \in \mathcal{L} \tag{9.14}$$

$$r^{\ell}_{\ell',\ell''} \leq 1 \qquad \ell, \ell', \ell''(\ell = \ell'') \in \mathcal{L} \tag{9.15}$$

$$\sum_{\ell \in \mathcal{E}(\mathcal{V}(\ell') \setminus \mathcal{V}(\ell''))} r^{\ell}_{\ell',\ell''} = 0 \qquad \ell', \ell'' \in \mathcal{L} \tag{9.16}$$

$$\sum_{\ell \in \mathcal{E}(v)} r^{\ell}_{\ell',\ell''} = 2n^{v}_{\ell',\ell''} \qquad v \in \mathcal{V}, \ell', \ell'' \in \mathcal{L} \tag{9.17}$$

where $n^{v}_{\ell',\ell''} \in \mathbb{Z}^{+}$ is a parameter.

Constraints (9.14) express that an alternate back path crosses only on-cycle links, and constraints (9.15) extend it to the second failing link. Constraint (9.16)-(ℓ', ℓ") removes link ℓ' and all its adjacent links that are not adjacent to ℓ''. Constraints (9.17) try to reconstruct a second p-cycle with the set of remaining links. This last set of constraints can be viewed as flow conservation constraints. Indeed, if a flow can circulate (while removing the first link and its adjacent links) from one of the two end-nodes of the second failing link and can reach the other end-node, then, it means that a disjoint backup path for the second failure can be established. If the reconstruction of a new p-cycle spanning ℓ'' succeeds, then the variable $r^{\ell''}_{\ell',\ell''}$ associated with the link ℓ'' will be equal to one. Thus, variable $r^{\ell''}_{\ell',\ell''}$ can be used to encode the feasibility of an alternate backup path for ℓ'' in case of removal of ℓ'.

Constraints (9.18) and (9.19) are used to set up variables $t_{\ell,\ell'}$ to a given value when the two links ℓ and ℓ' are both provided protection as straddling-cycle links. In case of a dual-link failure on ℓ and ℓ', constraints (9.18) set the amount of lost protected-capacity. In the particular case of $y^{s}_{\ell} = 1$ and $y^{s}_{\ell'} = 1$ (both ℓ and ℓ' have exactly one protected capacity), if it is not possible to reconstruct a second p-cycle without one of the failing links, constraints (9.19)-(ℓ, ℓ') will assign a value 1 to $t_{\ell\ell'}$, meaning, we cannot survive a dual-link failure on links ℓ and ℓ'.

$$t_{\ell.\ell'} \geq p_{\ell.\ell'}(y^{t}_{\ell} + y^{t}_{\ell'} - 2) \qquad \ell, \ell' \in \mathcal{L} \tag{9.18}$$

$$t_{\ell',\ell''} \geq p_{\ell,\ell'}(y^{t}_{\ell} + y^{t}_{\ell'} - r^{\ell''}_{\ell',\ell''} - 1) \quad \ell, \ell', \ell'' \in \mathcal{L}. \tag{9.19}$$

Last, in order to interconnect the master problem with the pricing problem, we need to express the variables of the pricing problems in terms of the variables of the master problem.

$$b^s_\ell = x^o_\ell \qquad \ell \in \mathcal{L}$$

$$a^s_\ell = y^o_\ell + y^t_\ell \qquad \ell \in \mathcal{L}$$

$$d^s_{\ell,\ell'} = t_{\ell,\ell'} \qquad \ell, \ell' \in \mathcal{L}.$$

Recall that, in case where all the $p_{\ell,\ell'} = 0$ ($\forall \{\ell, \ell'\} \in \mathcal{L}$) (dual-link failures cannot occur), the proposed model becomes a classical optimization model of a single-link failure survivable WDM network.

9.5.3 Optimized Design of p-Structure Based Protection Schemes

In this section, we extend the optimization approach proposed in the previous section for p-cycle protection to support all possible protection structures (p-structures).

Master problem

The master problem consists to minimize the spare capacity requirement in order to achieve the targeted QoP classes. It is written as follows:

$$\min \quad \sum_{s \in \mathcal{S}} \sum_{\ell \in \mathcal{L}} b^s_\ell z^s$$

Subject to:

$$\sum_{s \in \mathcal{S}} a^s_\ell z^s \geq w_\ell \qquad \ell \in \mathcal{L} \tag{9.20}$$

$$z^s \in \mathbb{Z}^+ \qquad s \in \mathcal{S}. \tag{9.21}$$

The only difference with the master problem of a p-cycle based scheme is in the set of Constraints 9.3. These constraints are moved into the pricing problem in the p-structure based scheme. Though, as opposed to the p-cycle model, the p-structure master model select among candidate p-structure which individually satisfies the targeted QoP, i.e., resilient against all failure scenarios in the network.

Pricing Problem

Based on the dual variables of the master problem, the pricing problem decides on the shape and the protection capability of each p-structure it generates.

We define the variables of the pricing problem as follows:

$$r^{\ell',\ell_j}_{\ell_1,\ell_2}(j \in \{1.2\}) = \begin{cases} 1 & \text{if } \ell' \text{ protect link } \ell_j \text{ in case of} \\ & \text{a dual-link failure on links } \ell_1, \ell_2 \\ 0 & \text{otherwise} \end{cases}$$

$$x_\ell = \begin{cases} 1 & \text{if } \ell \text{ is used for protection} \\ 0 & \text{otherwise} \end{cases}$$

$y_\ell \in \mathbb{Z}^+$ is the number of protected channels on link ℓ provided by the current p-structure.

The objective function of the pricing problem, i.e., minimization of the reduced cost of the master problem is deduced as follows:

$$\min \left(\sum_{\ell \in \mathcal{L}} b_\ell - \sum_{\ell \in \mathcal{L}} \theta_\ell a_\ell \right)$$

where $\theta_\ell(\ell \in \mathcal{L})$ are the dual variable values associated with constraints (9.20). Re-expressed the objective function in terms of the pricing variables leads to the following new expression:

$$\min \left(\sum_{\ell \in \mathcal{L}} x_\ell - \sum_{\ell \in \mathcal{L}} \theta_\ell y_\ell \right).$$

The constraints that shape and decide the protection capabilities of each p-structure are divided into two sets: the first set of constraints (9.22)-(9.24) are dual-link failure model dependent ($\mathcal{P}$ dependent). and the second set (9.25)-(9.30) is used to decide the protection capabilities and shape of each candidate p-structure.

$$\mathcal{P}_{\ell_1,\ell_2} \times r_{\ell_1,\ell_2}^{\ell_1,\ell_2} = 0 \qquad \ell_1, \ell_2, \in \mathcal{L} \tag{9.22}$$

$$\mathcal{P}_{\ell_1,\ell_2} \times r_{\ell_1,\ell_2}^{\ell_2,\ell_1} = 0 \qquad \ell_1, \ell_2 \in \mathcal{L} \tag{9.23}$$

$$\mathcal{P}_{\ell_1,\ell_2} \times (r_{\ell_1,\ell_2}^{\ell',\ell_1} + r_{\ell_1,\ell_2}^{\ell',\ell_2}) \leq 1 \qquad \ell_1, \ell_2, \ell' \in \mathcal{L}. \tag{9.24}$$

This set of constraints is used to avoid protection conflicts when links of any link-pair are susceptible to fail at the same time. Constraints (9.22) and (9.23) are used to forbid inter-link protection between any pair of links ℓ_1, ℓ_2 when they belong to the same SRLG (i.e., $\mathcal{P}_{\ell_1,\ell_2} = 1$). Indeed, if ℓ_1 and ℓ_2 are susceptible to fail at the same time ($\mathcal{P}_{\ell_1,\ell_2} = 1$), then, neither ℓ_1 can protect ℓ_2 i.e., $r_{\ell_1,\ell_2}^{\ell_1,\ell_2} = 0$, nor ℓ_2 can protect ℓ_1. i.e . $r_{\ell_1,\ell_2}^{\ell_2,\ell_1} = 0$). Constraints (9.24) are used to avoid for any link ℓ' to protect both of links ℓ_1, ℓ_2 of any SRLG when they are susceptible to fail at the same time ($\mathcal{P}_{\ell_1,\ell_2} = 1$) In such a case, ℓ' can only protect one of the two links.

$$\sum_{\ell'(\ell' \neq \ell_j) \in \mathcal{V}(N)} r_{\ell_1,\ell_2}^{\ell',\ell_j} \geq y_{\ell_j} \qquad N \subset \mathcal{V}, \ell_1, \ell_2 \in \mathcal{L}$$

$$\ell_j \in \{\ell_1, \ell_2\}, \tag{9.25}$$

$$r_{\ell_1 \ell_2}^{\ell_1,\ell_1} = 0 \qquad \ell_1, \ell_2, \in \mathcal{L} \tag{9.26}$$

$$r_{\ell_1 \ell_2}^{\ell_2 \ell_2} = 0 \qquad \ell_1. \ell_2 \in \mathcal{L} \tag{9.27}$$

$$r_{\ell_1 \ell_2}^{\ell' \ell_j} \leq x_{\ell'} \qquad \ell_1, \ell_2, \ell' \in \mathcal{L}, \ell_j \in \{\ell_1, \ell_2\} \tag{9.28}$$

$$r_{\ell_1 \ell_2}^{\ell',\ell_j} \in \{0, 1\} \qquad \ell_1, \ell_2, \ell' \in \mathcal{L}. \ell_j \in \{\ell_1. \ell_2\} \tag{9 29}$$

$$x_\ell \in \{0, 1\}, y_\ell \in \mathbb{Z}^+ \qquad \ell \in \mathcal{L}. \tag{9.30}$$

This second set of constraints. (9.25)-(9.30), is used to shape the p-structures, and decide for their protection. Constraints (9.25) are used for each link pair ℓ_1, ℓ_2 (either susceptible to fail at the same time or not) to set up the number of disjoint backup paths for link $\ell_j \in \{\ell_1, \ell_2\}$ to the minimum number of incident links to the minimum cut (min cut problem) separating the two end-nodes of ℓ_j. This technique was used in previous Chapters 7 and 8. Constraints (9.26) and (9.27) express that a link ℓ cannot protect itself. Constraints (9.28) say that a link ℓ' can provide protection for ℓ_j if and only if it (ℓ') is part of the current p-structure (spanned by the p-structure). Constraints (9.29) and (9.30) are integrality constraints.

9.6 Computational Results

By Menger's theorem [BM76], a graph is $k-$connected if and only if there are k edge-disjoint paths between every pair of nodes in the network. If so, the removal of any $k - n$ edges will leave the graph $n-$connected. In communication networks, in order to design a fully survivable dual-link failure scheme, the network physical topology must be at least 3-connected, i.e., all nodes (all sub networks) should have at least three incident disjoint-links (cuts of at least three-edges). In the performance evaluation processes, we use five network topologies, all at least 3-connected. Two highly connected: COST239 (11 nodes, 26 links, avg degree 4.3), an augmented version of the NJ-LATA (11 nodes, 26 links (3 added links), avg degree 4.2), and three relatively sparse: NSF (14 nodes, 22 links (one added link), avg degree 3.1), and ATLANTA (15 nodes, 24 links (two added links), avg degree of 3.2), and Polska [Zus] (12 nodes, 20 links (two added links), avg degree of 3.33).

In the next two sub-sections, we present the computation results of the pure p-cycle and the p-structure design approaches. Herein, we suppose uniform traffic distributions over the node-pairs in the network; and arbitrary link failure probability distributions.

9.6.1 p-Cycle Protection Performance

In Figure 9.9, we see the variation of the dual-link failure restorability as a function of the capacity redundancy (y-axis). The required amount of spare capacity to provide $R_2 = 100\%$ is about 2.3 the amount of protected capacity ($\sim$ 235% redundent) in both COST239 and NJ-LATA networks (highly connected networks). This redundancy decreases as the ratio of restorable dual-link failures drops down to achieve only 42% in case of a single failure scenario. The NSF and ATLANTA networks show the same behavior as for the previous two networks. However, the required amount of spare capacity to improve R_2 is growing faster for an equal increase of the R_2 ratio. The amount of spare capacity needed to achieve $R_2 = 100\%$ is about 5.2 the protected working capacity, and compared to the previous two networks the same amount that provides 100% dual-link failure protection in COST239 and NJ-LATA only provides around 20% dual-link failure protection in NSF and ATLANTA networks

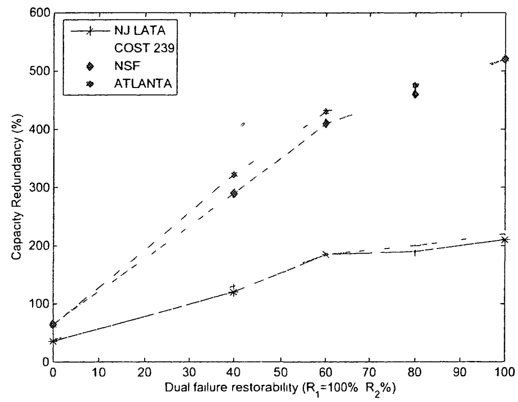


Figure 9.9· Redundancy vs. Dual-Link Failure Recovery Ratio R_2

The network physical topology does affect the ability of p-cycles in providing dual-link failure protection. Sparser networks offer less flexibility in the set up of p-cycles, which in turn, affects their capacity efficiency (fewer straddling-cycle links) and their ability to survive dual-link failures as well.

The second measured parameter is the average p-cycles size. The study performed in [Sch03b] showed the effect of varying the number of p-cycles on the capacity redundancy, and how varying the size of the candidate p-cycles could affect the restorability of a p-cycle based protection scheme. Figure 9.10 shows the variation of the average size of the p-cycles in the optimal design proposed in this study. The average size of the p-cycles that provides $R_1 = 100\%$. $R_2 \sim 0\%$ is larger than that at any other R_2 level

However, the drop in the average size is not that high. the average size of p-cycles providing 100% dual-link protection is only two hops less than that at $R_2 \sim 0\%$.

The physical topology also affects the size of the p-cycles in the optimal solution In the NSF

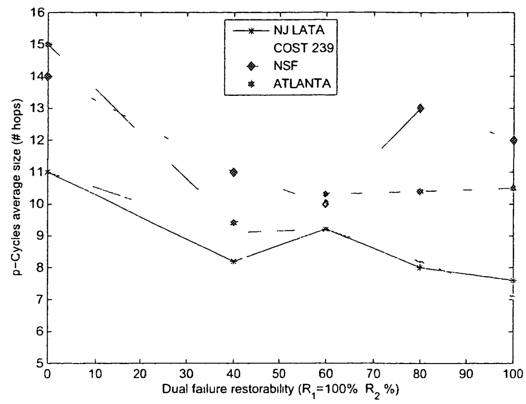


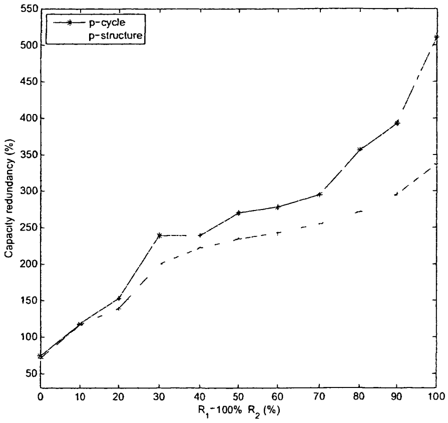
Figure 9.10: p-cycle Average Size vs. Dual-Link Failure Recovery Ratio R_2

and ATLANTA networks (sparse networks) much larger p-cycles (with a higher number of hops) are required in order to provide an optimized dual-link failure restorability (R_2). p-Cycles of large size are required even in the case of a lower dual-link failure restorability ratio ($R_2 = 40\%$). The same trend is observed in the NJ LATA and COST239 networks, but with less difference when the R_2 ratio changes.

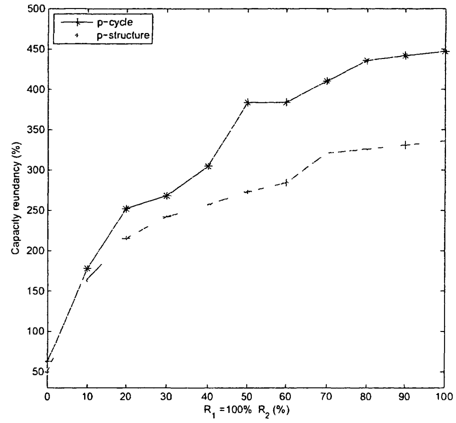
9.6.2 p-Structure Protection Performance

In Figure 9.11, we see the variation of the capacity redundancy (y-axis) as a function of the dual-link failure restorability (x-axis) in the p-cycle and p-structure schemes. We recorded a $\sim$ [3%. 5%] of protection capacity saving with the p-structure based scheme over the p-cycle one when the objective is to provide 100% single-link protection, i.e., $R_1 = 100\%$ and $R_2 = 0\%$ (origin of each plot) in all network topologies. The difference in spare capacity between the p-cycle and p-structure based schemes increases as the dual-link failure restorability increases

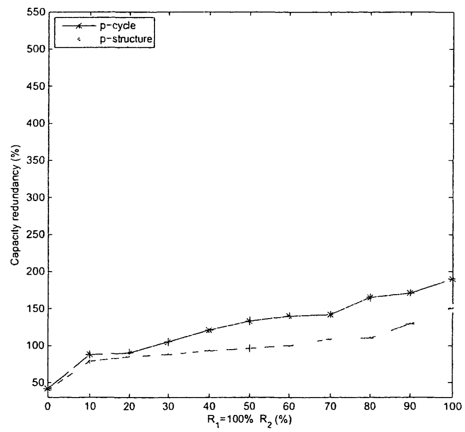
The required amount of spare capacity to provide $R_2 = 100\%$ in the p-cycle based scheme is $\sim$ 5.2 and 4.5 the amount of protected capacity ($\sim$ 520%. and $\sim$ 450% capacity redundant) in the NSF and Polska networks (relatively sparse networks). respectively The same $R_2 = 100\%$ level costs 150% and 100% less protection capacity when there is no constraint on the shape of the protection· structures (using p-structures). The saving in protection capacity related to the different R_2 levels in the p-structure over the p-cycle scheme varies in the interval [5%. 150%] and [5%. 100%] in the NSF and Polska networks, respectively. This difference is accentuated by the increasing level of R_2.



(a) NSF Network



(b) Polska Network



(c) COST239 Network

Figure 9.11: Capacity Redundancy vs. Dual-Link Failure Restorability

NSF and Polska networks are relatively sparser in comparison to COST239. Providing dual-link failure survivability even for a small class of traffic may cost excessively high when the network topology is sparse. COST239 offers a more effective support of dual-link failures with both the p-cycle and p-structure based schemes. Thanks to its physical connectivity, dual-link failures can be survived by rerouting the affected connections through diverse other protection paths. Furthermore, as there is no constraint on the shape of the protection structures in the (p-structures). this scheme is more likely to provide flexible and more efficient protection allocation than the p-cycle scheme The saving in protection capacity in this case lies in the interval $[5\%, 50\%]$.

In Tables 9.1 and (9 2), we present some additional characteristics related to the shapes of the

p-structures and p-cycles, respectively. We consider three R_2 levels: 10%, 50% and 100%, and two topologies: NSF and COST239.

In Table 9.1, we recorded the number of p-cycles and p-structures in the optimal solutions of the two designs for $R_2 = 10\%$, 50%, and 100%. We remark that the number of distinct p-cycles in both networks, and p-structures in the NSF network increases as the level of R_2 increases. The number of p-structures in COST239 network vary differently compared to others: for any R_2 level, this number is smaller than the number of required p-cycles. These variations come from the fact that when a higher number of SRLGs are assumed then larger number of distinct structures (especially sparse structures, e.g., p-cycles) are needed, especially in sparse networks (e.g., NSF network).

In Table 9.2, we study more in-depth the shapes and protection capabilities of the p-cycles and p-structures in the two proposed designs. We consider two statistic distributions: The number of spanned links and number of protected links by each p-cycle and p-structure The two distributions are characterized by $(\bar{\mathcal{X}}_{x_\ell}, \sigma_{x_\ell})$ and $(\bar{\mathcal{Y}}_{x_\ell}, \sigma_{y_\ell})$ which refer to their main value and standard deviation, respectively. We keep NSF and COST2309 networks, and the three previous R_2 levels i.e., 10%, 50%, and 100%.

In NSF, on average, the number of spanned links by the p-cycles and p-structures increase as the dual-link failure resiliency increases. Moreover, as R_2 increases, the p-structures tend to use slightly more links than the p-cycles do. Regarding the number of protected links in NSF network, the p-structures protect more working links than the p-cycles do. There is one exception, in the case $R_2 = 10\%$ where the difference in capacity between the p-structure and p-cycle schemes is $\sim 3\%$ (see Figure 9.11) and the average number of protected links by the p-cycles is larger than the p-structures. The standard deviations of the two distributions show a slightly larger discrepancy in the size (spanned links) and protected links between the p-structures and p-cycles There is a larger difference among the p-structures in terms of size and protected links than among the p-cycles. This discrepancy in size and protection explains the difference in protection performance in Figure 9.11 ($R_2 = 10$ in NSF) and in Table 9.2.

	$R_2 = 10\%$		$R_2 = 50\%$		$R_2 = 100\%$	
	NSF	COST239	NSF	COST239	NSF	COST239
p-cycle	12	16	19	19	20	22
p-structure	13	11	14	15	19	11

Table 9 1 Number of Protection Structures in the Optimal p-Cycle and p-Structure Schemes

	NSF Network											
	$R_2 = 10\%$				$R_2 = 50\%$				$R_2 = 100\%$			
	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{Y}}_{y_\ell}$	σ_{y_ℓ}	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{Y}}_{y_\ell}$	σ_{y_ℓ}	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{Y}}_{y_\ell}$	σ_{y_ℓ}
p–cycle	9 2	2 5	9 0	8 3	9 8	2 5	3 6	3 8	11 7	2 4	2 3	0 9
p–structure	9 0	3 6	7 9	8 7	10 6	3 5	4 6	4 3	13 0	4 2	3 9	2 0

	COST239 Network											
	$R_2 = 10\%$				$R_2 = 50\%$				$R_2 = 100\%$			
	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{Y}}_{y_\ell}$	σ_{y_ℓ}	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{X}}_{y_\ell}$	σ_{y_ℓ}	$\bar{\mathcal{X}}_{x_\ell}$	σ_{x_ℓ}	$\bar{\mathcal{Y}}_{y_\ell}$	σ_{y_ℓ}
p–cycle	8 4	1 6	8 2	4 0	9 6	1 2	6 4	1 7	10 2	1 2	5 3	1 0
p–structure	7 4	6 1	9 8	11 5	8 5	4 9	7 5	8 5	11 7	10 0	7 2	8 4

Table 9 2 Characterization of the Optimal p-Structures and p-Cycles

In COST239 network, the same trend is observed regarding the size of the p-cycles and p-structures (number of spanned links). The major difference with the NSF network is in the distributions of the protection and protected links of the p-cycles and p-structures. The size and number of protected-link discrepancies in the p-structure distributions are almost equal to the p-structure average size and to the average number of protected links by each p-structure, respectively. In other words, there are more different p-structures (larger and smaller) with different protection capabilities than p-cycles. The flexibility in capacity allocation and distribution offered by the p-structure scheme is better than the one offered by the p-cycle scheme, and this is corroborated by the protection capacity saving.

9.7 Conclusion

We proposed a design framework for link protection in survivable WDM networks based on p-cycles and p-structures in order to provide different measurable QoP classes including 100% single-link protection and different optimized dual-link failure protection R_2. We proposed the first optimization methods to design protection schemes to exactly (and optimally) measure the required spare capacity budget in p-cycle and p-structure schemes in order to provide different QoP guarantees. We evaluated the protection performance of the p-cycle and p-structure schemes, and provided a valued relationship between the required amount of spare capacity and the physical topology in order to achieve an optimized dual-link failure survivability. We also provided a valued relation among network connectivity, dual-link failure resiliency, and average size of the protection structures in the optimal designs.

CHAPTER 10

Conclusions and Future Work

10.1 Summary of Thesis

Differentiation of Quality-of-Recovery and Quality-of-Protection are two important features in the design of survivable WDM networks. In modern transport networks, the challenge related to optimization of the network resources to meet different service requirements has grown with the introduction of several new applications and services. In the design of protection schemes, the trade-off between sharing of protection capacity and the recovery delay has motivated many researchers of the community of survivable optical networks. These two protection parameters have generated some research in QoR and QoP differentiation in optical networks. Protection schemes based on dedicated to shared protection capacity have been proposed to differently optimize the recovery delay.

So far. not much work has been done in QoR and QoP differentiation in the optical layer using shared protection schemes. The prevalent design approach to optimize some protection parameters is based on protection schemes that use pre-defined shape protection structures to optimize some protection parameters. The pre-defined shape p-cycle scheme is a typical protection approach where the shape of the protection building blocks (cycles) define its potential protection performance. Indeed. because they are a priori capacity efficient and can be fully pre-cross connected ahead of failures. they have been widely studied in the design of protection schemes in the literature

[She06, KG05, GD02, Gru03, EM09, LS08, SGA02, SGC04b, ZY02a, AR08]. However, their a-priori efficiency can be offset by different network conditions, such as, traffic patterns and link spare capacity budgets. Indeed, because of the constraint on the shapes of the protection structures (cyclical), the flexibility in the set up of the protection capacity can be greatly jeopardized, which in turn can affect the efficiency of the protection scheme.

To overcome the above difficulties, in this dissertation, we proposed a set of new design approaches in order to effectively provide different classes of QoR and QoP. In the differentiation of QoR, we focused on the pre-configuration of the protection building blocks, and proposed different protection approaches that provide different recovery performances, and require different spare capacity budgets. We proposed three strategies to design protection schemes that are based on *fully pre-cross connected*, *partially pre-cross connected*, and *dynamically cross connected* protection structures. In the design of fully pre-cross connected schemes, we proposed two approaches using pre-defined shape p-cycles and unrestricted shape p-structures. In the p-cycle approach, the objective was to optimize the sharing of the protection capacity while keeping the fully pre-cross connectivity of the protection structures. The fully pre-cross connected p-structure based approach was proposed to overcome the limits related to the shapes of the p-cycles. In the design of dynamically cross connected schemes, we used p-structures as protection building blocks. In this approach, where the protection capacity is dynamically configured in case of a failure, the focus was more on how to reserve the protection capacity in order to provide protection with different constrained spare capacity budgets and traffic patterns. The partially pre-cross connected approach was proposed to strike a balance between the fully pre-cross connected and dynamically cross-connected protection schemes. In the design of partially pre-cross connected schemes, we proposed a hybrid protection structure, called *pre-configured extended-tree*, consisting of a p-tree and a set of potential p-cycles, and adapted the fully pre-cross connected p-structure based approach by relaxing the cross connectivity on some switching nodes. In the partially pre-cross connected p-structure approach, the number of cross connects that require dynamic reconfiguration at switching nodes and along backup paths, are explicitly optimized.

We used the three differently pre-configured protection approaches we proposed in this thesis in the design of protection schemes that guarantee different QoR classes in the context of Protected Working Capacity Envelope (PWCE) paradigm and the classical protected working capacity. In PWCE, we proposed efficient and scalable optimization techniques based on Column Generation (CG), and compared the required spare capacity and the provided reliability of the simple and non simple p-cycle, p-etree, and p-structure based schemes. The flexibility of these schemes in providing protection with non uniform link spare capacity budgets were also evaluated. In addition to the required spare capacity, we studied the recovery delay in the p-etree based scheme as a function of the number of cross connects that require dynamic reconfiguration in case of a link failure.

In the context of classical protected working capacity, we proposed optimization methods to explicitly optimize the number and distribution of dynamic cross connects at local nodes and along backup paths in the p-structure based schemes. By doing so, we limit the switching delay of light paths and the queuing delays of control messages, and though, can guarantee a short recovery delay independently of the shape of the protection structures.

In QoP differentiation, we used pure p-cycles and p-structures in the design of protection schemes that provide different QoP classes. We proposed two CG based optimization methods to *exactly* compute the spare capacity budget in order to provide different QoP classes including single and dual link failures. The associated spare capacity budget to provide different levels of dual link failure recovery were computed within different arbitrary dual link failure models. In both the p-cycle and p-structure based schemes, we focused on the shapes of the optimal p-cycles and p-structures. We recorded the size of the optimal p-cycles in different experiments with different QoP classes in order to get an insight of the relation between the size of the p-cycles and their resiliency. In the p-structure based scheme. we focused on the design of flexible protection structures to optimize the spare capacity, and looked at the shapes of those structures. We presented valuable information about the parameters defining the shapes of the protection structures in the designs of different protection schemes to provide different QoP classes.

10.2 Further Research

Further research can be done on the following topics:

10.2.1 Dynamic Provisioning within Different Shaped End-to-End PWCEs

In Chapter 7, we proposed a design method to maximize the protected-flow circulation in survivable WDM networks with p-structures-based PWCE. The objective was to shape the PWCE in order to effectively meet a potential working capacity pattern in the network. However, to be more flexible and efficient in tracking the traffic fluctuations, we can further extend this approach to a multi-PWCE approach where different shaped PWCEs will be designed to adapt to different traffic variations in the network. This approach can be built on the one presented in this thesis, p-structures. by extending the solution space of the PWCEs to include different inter-related PWCEs. All what it will take is a strategy to construct the PWCEs solution space, and an activation mechanism to select the most appropriate and effective PWCEs at each time a reconfiguration is needed Another interesting research direction would be to develop dynamic provisioning strategies in PWCE based on the p-etree scheme. The scalability and flexibility of this approach and the existence of a variety of distributed algorithms for tree construction, are valuable assets that can be exploited to efficiently and quickly allocate protection capacity on-demand in survivable WDM networks.

10.2.2 Path and Segment Based Protection Using p-Structures

All the design methods of PWCE and classical protection in this thesis were link-oriented. Path and segment based protection are two other approaches that are more capacity efficient than link protection [RSM03, XXQ03]. An interesting research direction to follow would be to generalize the design of p-structures in segment and path based protection schemes in order to provide different QoR and QoP classes. The challenges will be to extend the work done in this thesis, and to establish how the different protection parameters vary in each protection approach and according to each design objective. In the design of shaped PWCE, the segment and path based approaches will be of a great added value in saving the spare capacity required to maximize the PWCE size. In addition, in the shaping of the PWCEs, in order to maximize the protection flow circulation, the path and segment oriented protection approaches are more oriented to effectively maximize the end-to-end protection than the hop-by-hop counterpart.

10.3 Contributions of this Thesis Work

10.3.1 Journal Papers

1. **Sebbah, S.** Jaumard, B. Design of Survivable WDM Networks Using Pre-Configured Protection Structures with Unrestricted Shapes, Photonic Network Communications, Volume 19, Number 1 / February, 2010, pages=9-21

2. Jaumard, B. **Sebbah, S.** Stidsen, T. A unified modeling and solution framework to pre-planned protection in survivable WDM networks, International Journal On Communications (under review)

3. **Sebbah, S.** Jaumard, B. Differentiated Quality-of-Recovery in Survivable WDM Mesh Networks with p-Structures, IEEE/ACM Journal on Networking (under review)

4. **Sebbah, S.** Jaumard, B. Differentiated Quality-of-Protection in Survivable WDM Mesh Networks with p-Structures, IEEE/OSA Journal of Optical Communications and Networking (JOCN) (under review)

10.3.2 Peer-Reviewed Conference Papers

1. **Sebbah, S.** Jaumard, B. A Global Approach to Fully Pre-cross Connected Protection Schemes Design using p-structures, IEEE International Workshop on Reliable Networks Design and Modeling, 2009. RNDM'09. St Petersburg, Russia. pages=1-6.

2. **Sebbah, S.** Jaumard. B. Differentiated Quality-of-Service in Survivable WDM Mesh Networks, Global Telecommunications Conference. 2009. GLOBECOM 2009. Hawaii, USA. page(s): 1 - 6

3. Jaumard, B. **Sebbah, S.** Rocha, C. Large Scale optimization in Survivable WDM Networks, *Tutorial*, IEEE Design of Reliable Communication Networks, 2009. (DRCN'09). Pittsburgh, USA.

4. **Sebbah, S.** Jaumard, B. A Resilient Transparent Optical Network Design with a Pre-configured Extended-tree Protection, IEEE International Conference on Communications, 2009, (ICC'09) Dresden, Germany. pages=1-6. (**Received the best paper award of the Optical Networks Symposium**).

5. **Sebbah, S.** Jaumard, B. Flexible protection plans design in survivable WDM networks: An application to PWCE, IEEE Sarnoff 2009. Princeton. NJ. USA. pages =1–5.

6. **Sebbah, S.** Jaumard, B. PWCE design in survivable WDM Networks using unrestricted shape p-structure patterns, IEEE 22^{nd} Canadian Conference on Electrical and Computer Engineering 2009 (CCECE'09). pages = 279 - 282.

7. **Sebbah, S.** Jaumard, B p-Cycle Based Dual Failure Recovery in WDM Mesh Networks. IFIP / IEEE 13^{th} Conference on Optical Network Design and Modeling 2009. (ONDM'09). Braunschweig, Germany. pages=1–6.

8. **Sebbah, S.** Jaumard, B. Survivable WDM networks design with non-simple p-cycle-based PWCE, IEEE Global Communications Conference, 2008. (GLOBECOM'08). New Orleans, LA, USA. pages=1–6.

9. **Sebbah, S.** Jaumard, B. Efficient and Scalable Design of Protected Working Capacity Envelope, 13^{th} International Telecommunications Network Strategy and Planning Symposium Budapest, Hungary. pages=1-21.

Bibliography

[AKM03] S. Arakawa, J. Katou, and M. Murata. Design method of logical topologies with quality of reliability in WDM networks. Photonic Network Communications, 5(2):107–121, 2003.

[AMO93] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin. Network Flows: Theory, Algorithms and Applications. Prentice Hall, 1993.

[AR08] A. Atamtürk and D. Rajan. Partition inequalities for capacitated survivable network design based on directed p-cycles. Discrete Optimization, 5:415–433, 2008.

[ASBB+01] P. Ashwood-Smith, A. Banerjee, L. Berger, G. Bernstein, J. Drake, Y. Fan, K. Kompella, E. Mannie, J. P. Lang, and *et al.* Generalized MPLS-signaling fuctional description. draft-ietf-mpls-generalized-signaling-07.txt, November, 2001.

[Bal96] G. Balbe *et al.* Operator requirements. Technical report, European ACTS project Protection Across Network Layers (PANEL), December 1996.

[BDH+00] P. Batchelor, B. Daino, P. Heinzmann, D.R. Hjelme, R. Inkret, H.A. Jager, M. Joindot, A. Kuchar, E.L. Coquil, P. Leuthold, et al. Study on the implementation of optical transparent transport networks in the european environment—results of the research project cost 239. Photonic Network Communications, 2(1).15–32. 2000.

[Ber03a] L. Berger *et al.* Generalized MPLS Signaling-RSVP-TE Extensions. RFC3473. January. 2003.

[Ber03b] L. Berger *et al.* Generalized multi-protocol label switching (GMPLS) signaling functional description. RFC 3471, January 2003, 2003.

[BJN+98] C. Barnhart, E. L. Johnson, G. L. Nemhauser, M. W. P. Savelsbergh, and P.H. Vance. Branch-and-price: Column generation for solving huge integer programs. Operations Research, 46(3):316–329, May-June 1998.

[BJS08] M. S. Bazaraa, J. J. Jarvis, and H. D. Sherali. Linear programming and network flows. Wiley India Pvt. Ltd., 2008.

[BKLS01] E. Bouillet, K. Kumaran, G. Liu, and I. Saniee. Wavelength usage efficiency versus recovery time in path-protected DWDM mesh networks. In Optical Fiber Communication Conference - OFC, volume 2, 2001

[BM76] J.A. Bondy and U.S.R. Murty. Graph theory with applications. MacMillan London, 1976.

[BM96] D. Banerjee and B. Mukherjee. A practical approach for routing and wavelength assignment in large wavelength-routed optical networks. IEEE Journal on Selected Areas in Communications, 14(5):903–908, 1996.

[BRS03] G. Bernstein, B. Rajagopalan, and D. Saha. Optical network control: architecture, protocols, and standards. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 2003.

[CCF04a] T. Chow, F. Chudak, and A. Ffrench. Fast optical layer mesh protection using pre-cross-connected trails. IEEE/ACM Transactions on Networking, 12(3):539–548. 2004.

[CCF04b] T. Y. Chow, F. Chudak, and A. M. Ffrench. Fast optical layer mesh protection using pre-cross-connected trails. IEEE/ACM Transactions on Networking (TON), 12(3):539–548, 2004.

[CF97] A. Caprara and M. Fischetti. Branch-and-Cut algorithms. Annotated Bibliographies in Combinatorial Optimization, pages 45–63, 1997.

[CFZ96] I. Chlamtac, A. Farago, and T. Zhang. Lightpath (wavelength) routing in large WDM networks. IEEE Journal on Selected Areas in Communications, 14(5):909–913, 1996.

[CG05] M. Clouqueur and W.D. Grover. Mesh-restorable networks with enhanced dual-failure restorability properties. Photonic Network Communications, 9(1):7–18, 2005.

[Chv83] V. Chvátal. Linear Programming. Freeman, 1983.

[CLB98] O. Crochat and J.Y. Le Boudec. Design protection for WDM optical networks. IEEE Journal on Selected Areas in Communications, 16(7):1158–1165, 1998.

[Col87] C. J. Colbourn. The Combinatorics of Network Reliability. Oxford University Press, 1987.

[CP99a] Z.L. Chen and W.B. Powell. A column generation based decomposition algorithm for a parallel machine just-in-time scheduling problem. European Journal of Operational Research, 116(1):220–232, 1999.

[CP99b] Z.L. Chen and W.B. Powell. Solving parallel machine scheduling problems by column generation. INFORMS Journal on Computing, 11:78–94, 1999.

[CSC02] H. Choi, S. Subramaniam, and H.A. Choi. On double-link failure recovery in WDM optical networks. In IEEE Annual Joint Conference of the IEEE Computer and Communications Societies - INFOCOM, volume 2, 2002.

[D'A09] J. D'Amborsia. 40 gigabit Ethernet and 100 gigabit Ethernet: the development of a flexible architecture. IEEE Communications Magazine, page s10, 2009.

[Dan98] G.B. Dantzig. Linear programming and extensions. Princeton University Press, 1998.

[DDS05] G. Desaulniers, J. Desrosiers, and M. M. Solomon, editors. Column Generation, GERAD 25th Anniversary Series. Spring, 2005.

[Dem99] P. Demeester *et al.* Resilience in a multi-layer network. IEEE Communication Magazine, 37(8):70–76, Aug 1999.

[DHGY03] J. Doucette, D. He, W. D Grover, and O. Yang. Algorithmic approaches for efficient enumeration of candidate p-cycles and capacitated p-cycle network design. In Proceedings of Fourth International Workshop on Design of Reliable Communication Networks (DRCN), pages 212–220, 2003.

[Dij59] E.W. Dijkstra. A note on two problems in connexion with graphs. Numerische mathematik, 1(1):269–271, 1959.

[DP84] N. Deo and C. Pang. Shortest path algorithms: Taxonomy and annotation. Networks, 14(2):275–323, 1984.

[DS89] M. Desrochers and F. Soumis. A column generation approach to the urban transit crew scheduling problem. Transportation Science, 23(1):1, 1989.

[DSST99] R. D. Doverspike, G. Sahin, J. L. Strand, and R. W. Tkach. Fast restoration in a mesh network of optical cross-connects. In Optical Fiber Communication Conference - OFC, volume 1, 1999.

[EHS00] G. Ellinas, A. G. Hailemariam, and T. E. Stern. Protection cycles in mesh WDM networks. IEEE J. Selected Areas of Communications, 8:1924–1937, October 2000.

[EM09] A. E. Eshoul and H. T. Mouftah. Survivability approaches using p-cycles in WDM mesh networks under static traffic. IEEE/ACM Transactions on Networking (TON), 17(2):671–683, April 2009.

[Epp99] D. Eppstein. Finding the k shortest paths. SIAM Journal of Computing, 28(2):652–673, 1999.

[FB06] A. Farrel and I. Bryskin. GMPLS: architecture and applications. Morgan Kaufmann, 2006.

[FCC96] FCC. Telecommunications act of 1996. http://www.fcc.gov/telecom.html, 1996.

[Flo62] R.W. Floyd. Algorithm 97: shortest path. Communications of the ACM, 5(6):345, 1962.

[GC05] W.D. Grover and M. Clouqueur. Span-restorable mesh networks with multiple quality of protection (QoP) service classes. Photonic Network Communications, 9(1):19–34, January 2005.

[GCM+03] A. Groebbens, D. Colle, S. De Maesschal, I. Lieven, M. Pichavet, P. Demeester, L. Tran, K. Steenhaut, and A. Nowé. Efficient protection in MPλS networks using backup trees: part-One concepts and heuristics. Photonic Network Communications, 6(3):191–206, 2003.

[GD02] W. D. Grover and J. Doucette. Advances in Optical Network Design with p-Cycles. In IEEE LEOS Summer Topicals Meeting, 2002.

[GG07] A. Grue and W. Grover. Comparison of p-cycles and p-trees in a unified mathematical framework. Photonic Network Communications, 14(2):123–133, 2007.

[GM00] W.D. Grover and R.G Martens. Optimized design of ring-mesh hybrid networks. In Proceedings of IEEE/VDE Workshop on Design of Reliable Communication Networks (DRCN), pages 291–297, Munich, Germany, April April 2000.

[GR00a] O. Gerstel and R. Ramaswami. Optical layer survivability: A services perspective. IEEE Communications Magazine, 38(3):104–113, 2000.

[GR00b] O. Gerstel and R. Ramaswami. Optical layer survivability an implementation perspective. IEEE Selected Areas in Communications, 18:1885–1899, October 2000.

[Gro04a] W. D. Grover. Mesh-Based Survivable Networks. Prentice-Hall, 2004.

[Gro04b] W. D. Grover. The protected working capacity envelope concept: An alternative paradigm for automated service provisioning. IEEE Communications Magazine, 42(1):62–69, 2004.

[GRS98] O. Gerstel, R. Ramaswami. and G.H. Sasaki. Fault tolerant multiwavelength optical rings with limited wavelength conversion. IEEE Journal on Selected Areas in Communications. 16(7):1166–1178, 1998.

[Gru03] C. G. Gruber. Resilient networks with non-simple p-cycles. In Proceedings of International Conference on Telecommunication (ICT 2003), volume 2, pages 1027–1032, 2003.

[Gry04] M. Gryseels. Planning of multi-technology telecommunication networks. PhD thesis, Ghent University, Ghent, Belgium, January 2004.

[GS98] W.D. Grover and D. Stamatelakis. Cycle-oriented distributed pre-configuration: ring-like speed with mesh-like capacity for self-planning network restoration. In IEEE International Conference on Communications (ICC 1998), volume 1, pages 537–543, 1998.

[GS00] W. D. Grover and D. Stamatelakis. Bridging the ring-mesh dichotomy with p-cycles. In Proceedings of IEEE/VDE Workshop on Design of Reliable Communication Networks - DRCN, pages 92–104, Munich, Germany, April 2000.

[GS02] O. Gerstel and G. Sasaki. Quality of protection (QoP): A quantitative unifying paradigm to protection service grades. Optical Networks Magazine, 3(3):40–49, 2002.

[GS03] W. D. Grover and G. Shen. Extending the p-cycle concept to path-segment protection. In IEEE International Conference on Communications (ICC), pages 1314–1319, 2003.

[Hec98] J. Hecht. Understanding fiber optics. Prentice-Hall, Inc. Upper Saddle River, NJ, USA, 1998.

[HLS07] C.C. Huang, M.Z. Li. and A. Srinivasan. A scalable path protection mechanism for guaranteed network reliability under multiple failures. IEEE Transactions on Reliability, 56:254–267, June 2007.

[HM02] P.-H. Ho and H. T. Mouftah. A framework for service-guaranteed shared protection in WDM mesh networks. IEEE Communications Magazine, pages 97–103, February 2002.

[HM04] P.-H. Ho and H. T. Mouftah. A novel survivable routing algorithm for segment shared protection in mesh WDM networks with partial wavelength conversion. IEEE Journal of Selected Areas on Communications (JSAC), 22(8):1539–1548, 2004.

[HS03] W. He and A.K. Somani. Path-based protection for surviving double-link failures in mesh-restorable optical networks. GLOBECOM, 5:2558–2563, 2003.

[HS07] W. He and A. Somani. Comparison of protection mechanisms: Capacity efficiency and recovery time. In IEEE International Conference on Communications - ICC, pages 2218–2223, 2007.

[ILO03] ILOG Inc., Gentilly, France. CPLEX 9.0 User's Manual, 2003.

[ITR94] E.800 ITU-T Recommendation. Terms and definitions related to quality of service and network performance including dependability. ITU-T Standardization Organization, August 1994.

[JM98] I. Jurdana and B. Mikac. An availability analysis of optical cables. In Workshop on All-Optical Networks-WAON 98, 1998.

[JRBG07] B. Jaumard. C. Rocha, D. Baloukov, and W. D. Grover. A column generation approach for design of networks using path-protecting p-cycles. In Proceedings of IEEE/VDE Workshop on Design of Reliable Communication Networks - DRCN, October 2007.

[JRT95] M. Jünger, G. Reinelt, and S. Thienel. Practical problem solving with cutting plane algorithms in combinatorial optimization. Combinatorial optimization. papers from the DIMACS Special Year, page 111, 1995.

[JT98] M. Jünger and S. Thienel. Introduction to ABACUS a branch-and-cut system. Operations Research Letters. 22(2-3):83–95, 1998.

[KCY+03] I. Keslassy, S.T. Chuang. K. Yu. D. Miller, M. Horowitz. O. Solgaard. and N. McKeown. Scaling internet routers using optics. In Proceedings of the 2003 conference on

Applications, technologies, architectures, and protocols for computer communications, page 200. ACM, 2003.

[KG05] A. Kodian and W.D. Grover. Failure-independent path-protecting p-cycles: efficient and simple fully pre-connected optical-path protection. Journal of lightwave technology, 23(10):3241, 2005.

[KJ60] JE Kelley Jr. The cutting-plane method for solving convex programs. Journal of the Society for Industrial and Applied Mathematics, 8(4):703–712, 1960.

[KL00] M.S. Kodialam and T.V. Lakshman. Dynamic routing of bandwidth guaranteed tunnels with restoration. In INFOCOM, volume 2, pages 902–911, March 2000.

[KL03] M. Kodialam and TV Lakshman. Dynamic routing of restorable bandwidth-guaranteed tunnels using aggregated network resource usage information. IEEE/ACM Transactions on Networking (TON), 11(3):399–410, 2003.

[Kuh97] D.R. Kuhn. Sources of failure in the public switched telephone network. Computer, 30(4):31–36, 1997.

[Las70] L. S. Lasdon. Optimization Theory for Large Systems. MacMillan, New York, 1970.

[LD05] M. E. Lübbecke and J. Desrosiers. Selected topics in column generation. Operations Research, 53:1007–1023, 2005.

[LDK01] G. Li, R. Doverspike, and C. Kalmanek. Fiber span failure protection in mesh optical networks. In Proceedings of SPIE, volume 4599. page 130, 2001.

[LE98] E. Lowe and B. Eng. Current european WDM deployment trends. IEEE Communications Magazine, 36(2):46–50. 1998.

[LR06] C. Liu and L. Ruan. Dynamic provisioning of survivable services using path-segment protecting p-cycles in WDM networks. In IEEE International Conference on Computer Communication Networks - ICCCN. pages 275–280, October 2006.

[LS08] D. Lastine and A. Somani. Supplementing non-simple p-cycles with preconfigured lines. In IEEE International Conference on Communications - ICC, pages 5443–5447, 2008.

[LW66] E.L. Lawler and D.E. Wood. Branch-and-bound methods: A survey. Operations Research, 14(4):699–719, 1966.

[LYSH03] H. Liu, O. Yang, and S. Shah-Heydari. A tree-based link protection algorithm. In Canadian Conference on Electrical and Computer Engineering - IEEE CCECE, volume 2, pages 939 – 942, 2003.

[LYWK02] G. Li, J. Yates, D. Wang, and C. Kalmanek. Control plane design for reliable optical networks. IEEE Communications Magazine, 40(2):90–96, 2002.

[M+04] E. Mannie et al. Generalized multi-protocol label switching architecture. RFC3945, October, 2004.

[Mae98] M. W. Maeda. Management and control of transparent optical networks. IEEE Journal on Selected Areas in Communications, 16(7):1008–1023, 1998.

[MBF+02] M. Médard, R.A. Barry, S.G. Finn. W He. and S S. Lumetta. Generalized loop-back recovery in optical mesh networks. IEEE/ACM Transactions on Networking (TON), 10(1):153–164, 2002.

[MCL+03] S.D. Maesschalck, D. Colle, I. Lievens, M. Pickavet, P. Demeester, C. Mauz, M. Jaeger, R. Inkret. B. Mikac, and J. Derkacz. Pan-european optical transport networks: an availability-based comparison. Photonic Network Communications. 5(3):203–225. 2003.

[MFB99] M. Medard, S.G Finn, and R.A. Barry. Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs IEEE/ACM Transactions on Networking (TON), 7(5):641–652, 1999.

[MK97] K. Murakami and H. S. Kim. Comparative study on restoration schemes of survivable ATM networks. In INFOCOM. pages 345–352. 1997.

[MK03] X. Ma and G.S. Kuo. Optical switching technology comparison: optical MEMS vs. other technologies. IEEE Commun. Mag, 41(11):16–23, 2003.

[Muk92a] B. Mukherjee. WDM-based local lightwave networks. I. single-hop systems. Network, 6(3):12–27, May 1992.

[Muk92b] B. Mukherjee. WDM-based local lightwave networks. II. multi-hop systems. Network, 6(4):20–32, July 1992.

[NBWS04] S. Norden, M.M. Buddhikot, M. Waldvogel, and S. Suri. Routing bandwidth-guaranteed paths with restoration in label-switched networks. Computer Networks, 46(2):197–218, 2004.

[NR06] T.F. Noronha and C.C. Ribeiro. Routing and wavelength assignment by partition coloring. European Journal of Operational Research, 171(3):797–810, 2006.

[NW88] George L. Nemhauser and Laurence A. Wolsey. Integer and Combinatorial Optimization. Wiley, New York, 1988.

[NW99] G. L. Nemhauser and L. A. Wolsey. Integer and Combinatorial Optimization. Wiley, 1999.

[Ogt02] O. Ogtildeuz. Generalized column generation for linear programming. Management Science, 48(3):444–452, March 2002.

[OM04] C. Ou and B. Mukherjee. Differentiated quality-of-protection provisioning in optical/MPLS networks. Lecture notes in computer science, pages 650–661, 2004.

[OZZ+04] C. Ou, J. Zhang, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee. New and improved approaches for shared-path protection in WDM networks. IEEE/OSA, J. Lightwave of Technology, 22:1223–1232, May 2004.

[PM04] M. Pióro and D. Medhi. Routing, flow, and capacity design in communication and computer networks. Morgan Kaufmann Publishers. 2004.

[RC08] S. Ramasubramanian and A. Chandak. Dual-link failure resiliency through backup link mutual exclusion. IEEE/ACM Transactions on Networking (TON), 16(1):157–169, 2008.

[Rec01] I. Rec. G. 8080/Y.1304". Architecture for the Automatically Switched Optical Network (ASON), 2001.

[RI98] J. P. Ryan and R.H.K. Inc. WDM: North American deployment trends. IEEE Communications Magazine, 36(2):40–44, 1998.

[RJ08] C. Rocha and B. Jaumard. Revisiting p-cycles / FIPP p-cycles vs. shared link / path protection. In IEEE International Conference on Computer Communication Networks - ICCCN, pages 1–6, 2008.

[RM99] S. Ramamurthy and B. Mukherjee. Survivable WDM mesh networks - Part I. protection. In INFOCOM, volume 2, 1999.

[RPS+00] B. Rajagopalan, D. Pendarakis, D. Saha, R.S. Ramamoorthy, and K. Bala. IP over optical networks: Architectural aspects. IEEE Communications Magazine, 38(9):94–102, 2000.

[RS94] C.C. Ribeiro and F. Soumis. A column generation approach to the multiple-depot vehicle scheduling problem. Operations Research, pages 41–52, 1994.

[RSM03] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee. Survivable WDM mesh networks. Journal of Lightwave Technology, 21(4):870, 2003.

[RSS09] R. Ramaswami, K. Sivarajan, and G. H. Sasaki. Optical Networks: A Practical Perspective. Morgan Kaufmann, 3 edition, 2009.

[RT05] L. Ruan and F. Tang. Dynamic establishment of restorable connections using p-cycle protection in WDM networks. In International Conference on Broadband Networks, volume 1, pages 137 – 144, October 2005.

[Sch98] A. Schrijver. Theory of linear and integer programming. John Wiley & Sons Inc, 1998.

[Sch02] D. A. Schupke. Off-line lightpath routing in WDM networks with different wavelength converter configurations. In Workshop on High Performance Switching and Routing (HPSR). Workshop on Merging Optical and IP Technologies, pages 283–288. IEICE/IEEE, 2002.

[Sch03a] D. A. Schupke. Multiple failure survivability in WDM networks with p-cycles. In Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, volume 3, 2003.

[Sch03b] D. A. Schupke. The tradeoff between the number of deployed p-cycles and the survivability to dual fiber duct failures. In Communications, 2003. ICC'03. IEEE International Conference on, volume 2, 2003.

[SG99] D. Stamatelakis and W. D. Grover. Network restorability design using pre-configured trees, cycles, and mixture of pattern types. Technical Report TR-1999-05, TRLabs Technical Report, 1999.

[SG00] D. Stamatelakis and W. D. Grover. Theoretical underpinnings for the efficiency of restorable networks using pre-configured cycles (p-cycles). IEEE Trans. Commu, 48(8):1262–1265, 2000.

[SG03a] G. Shen and W. D. Grover. Exploiting forcer structure to serve uncertain demands and minimize redundancy of p-cycle networks. In Proc. 4th international Conference on Optical Networking and Communications (OptiComm 2003), volume 5285, pages 59–70, October 2003.

[SG03b] G. Shen and W. D. Grover. Extending the p-cycle concept to path segment protection for span and node failure recovery. IEEE Journal on Selected Areas in Communications, 21(8):1306–1319, October 2003.

[SG03c] G. Shen and W.D. Grover. Extending the p-cycle concept to path-segment protection for span and node failure recovery. IEEE Journal on Selected Areas in Communications, 21(8):1306–1319, Oct 2003.

[SG04a] G. Shen and W. Grover. Segment-based approaches to survivable translucent network design under various ultra-long-haul system reach capabilities [Invited]. Journal of Optical Networking, 3(1):1–24, 2004.

[SG04b] G. Shen and W. D. Grover. Performance of protected working capacity envelopes based on p-cycles: fast, simple, and scalable dynamic service provisioning of survivable services. In Proceedings of APOC, volume 5626, pages 519–533, 2004.

[SG05] G. Shen and W. D. Grover. Design and performance of protected working capacity envelopes based on p-cycles for dynamic provisioning of survivable services. Journal of Optical Networking, 4:361–390, July 2005.

[SGA02] D. A. Schupke, C. G. Gruber, and A. Autenrieth. Optimal configuration of p-cycles in WDM networks. In IEEE International Conference on Communications - ICC, volume 5, pages 2761–2765, May 2002.

[SGC04a] D. A Schupke, W. D Grover, and M Clouqueur. Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks. In Communications, 2004 IEEE International Conference on, volume 3, 2004.

[SGC04b] D. A. Schupke, W. D. Grover, and M. Clouqueur. Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks. In IEEE International Conference on Communications - ICC. volume 3, pages 1628– 1633, June 2004.

[SGM93] J.B. Slevinsky, W.D. Grover, and M.H. MacGregor. An algorithm for survivable network design employing multiple self-healing rings. In IEEE Global Telecommunications Conference, GLOBECOM'93., pages 1568–1573, 1993.

[SGZ04] C. V. Saradhi, M. Gurusarny, and L. Zhou. Differentiated QoS for survivable WDM optical networks. IEEE Communications Magazine, 42(5):S8–14, 2004.

[SH03] V. Sharma and F. Hellstrand. Framework for multi-protocol label switching (MPLS)-based recovery. RFC 3469, February 2003, 2003.

[She06] G. Shen. Design and performance of protected working capacity envelopes based on p-cycles: an alternative framework for dynamic survivable network service provisioning. PhD thesis, University of Alberta, 2006.

[SHY04] S. Shah-Heydari and O. Yang. Hierarchical protection tree scheme for failure recovery in mesh networks. Photonic Network Communications, 7(2):145–149, 2004.

[SHY09] S. Shah-Heydari and O. Yang. Heuristic algorithms for designing self-repairing protection trees in mesh networks. Computer Networks, 53(14):2537–2551, 2009.

[Sim07] J M. Simmons. Cost vs. capacity tradeoff with shared mesh protection in optical-bypass-enabled backbone networks. In Optical Fiber Communication and the National Fiber Optic Engineers Conference, 2007. OFC/NFOEC 2007. Conference on, pages 1–9, 2007.

[SM04] C. V. Saradhi and C. S. R. Murthy. Dynamic establishment of differentiated survivable lightpaths in WDM mesh networks. Computer Communications, 27(3):273–294, 2004.

[SPR+07] T. Stidsen, B. Petersen, K.B. Rasmussen, S. Spoorendonk, M. Zachariasen, F. Rambach, and M. Kiese. Optimal routing with single backup path protection. In Proceedings of the 3^{rd} International Network Optimization Conference (INOC 2007), Spa, Belgium, 2007.

[SR01] S Sengupta and R. Ramamurthy. Capacity efficient distributed routing of mesh-restored lightpaths in optical networks. In Proceedings of IEEE Global Telecommunications Conference (GlobeCom 2001), pages 2129–2133, San Antonio, TX, November 2001.

[SRB03] D. Saha, B. Rajagopalan, and G. Bernstein. The optical network control plane: state of the standards and deployment. IEEE Commun Mag, 41, 2003.

[SS04] G. Sahin and S. Subramaniam. Providing quality-of-protection classes through control-message scheduling in DWDM mesh networks with capacity sharing. IEEE Journal on Selected Areas in Communications, 22(9):273–294, 2004.

[SSM03] N.K. Singhal, L.H. Sahasrabuddhe, and B. Mukherjee. Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks. Journal of lightwave technology, 21(11):2587, 2003.

[Sum05] S. Sumner. http://www.exfo.com/en/library/wavereview/2005-april/wrarticle2.asp, 2005.

[SYR03] L. Shen, X. Yang, and B. Ramamurthy. Shared-risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks: Formulation and solution approaches. In Proceedings of the SPIE OptiComm 2003, volume 5285, pages 126–138, 2003.

[SYR05] L. Shen, X. Yang, and B. Ramamurthy. Shared risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks. IEEE/ACM Transactions on Networking, 13:918 – 931, August 2005.

[SZM05] L. Song, J. Zhang, and B. Mukherjee. Dynamic provisioning with reliability guarantee and resource optimization for differentiated services in WDM mesh networks. In Optical Fiber Communication Conference (OFC), 2005.

[SZZW07] X. Shao, L. Zhou, W. Zheng, and Y. Wang. Providing differentiated quality-of-protection for surviving double-link failures in WDM mesh networks. In IEEE International Conference on Communications, 2007. ICC'07, pages 2180–2185, 2007.

[THV+08] J. Tapolcai. P.-H. Ho, D. Verchre, T. Cinkler, and A. Haque. A new shared segment protection method for survivable networks with guaranteed recovery time. IEEE Transactions on Reliability, 57:272–282, June 2008.

[TMP05] M. Tornatore, G. Maier, and A. Pattavina. Availability design of optical transport networks. IEEE Journal on Selected Areas in Communications, 23(8):1520–1532, 2005.

[TN94] M. To and P Neusy. Unavailability analysis of long-haul networks. IEEE J. Selected Areas of Communications, 12(1):100–109, January 1994.

[TT05] F. Tang and L. Tuan. A protection tree scheme for first failure protection and second failure restoration in optical networks. In Proceedings of International Conference on Computer Network and Mobile Computing, volume 3619, pages 620–631, August 2005.

[Uni01] International Telecommunication Union. Architecture of optical transport networks. ITU-T Rec. G 872, November 2001.

[Uni03] International Telecommunication Union. Interfaces for the optical transport network (OTN), ITU-T Rec. 709, March 2003.

[Van94] F. Vanderbeck. Decomposition and column generation for integer programs. PhD thesis, Université catholique de Louvain, 1994.

[Van00] F. Vanderbeck. On Dantzig-Wolfe decomposition in integer programming and ways to perform branching in a branch-and-price algorithm. Operations Research, 48(1):111–128, 2000.

[Van06] F. Vanderbeck. Branching in branch-and-price: a generic scheme. Report, University Bordeaux I, 2006.

[VBJ+98] P Vance, C. Barnhart, E. L. Johnson, G. L. Nemhauser, and M. Savelsbergh. Branch-and-price: column generation for huge integer programs. Operations Research, 46(3):316–329, 1998.

[VPD04] J. P. Vasseur, M. Pickavet, and P. Demeester. Network recovery: protection and restoration of optical, SONET-SDH, IP, and MPLS Morgan Kaufmann, San Francisco, CA, 2004.

[VW96] F. Vanderbeck and L. A. Wolsey. An exact algorithm for IP column generation. Operational Research Letter, 19:151–157, 1996.

[WAPD01] G. Willems, P. Arijs, W. V. Parys, and P. Demeester. Capacity vs. availability trade-offs in mesh-restorable WDM networks. In International Workshop on the Design of Reliable Communication Networks (DRCN), 2001.

[Wol00] L. A. Wolsey. Integer programming. IIE Transactions, 32:273–285, 2000.

[WSM02] J. Wang, L. Sahasrabuddhe, and B. Mukherjee. Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signaling. IEEE Communications Magazine, 40:80–82, November 2002.

[Wu92] T. H. Wu. Fiber network service survivability. Artech House. Inc. Norwood. MA, USA, 1992.

[XCT03] G. Xue, L. Chen. and K. Thulasiraman. Quality-of-service and quality-of-protection issues in preplanned recovery schemes using redundant trees. IEEE Journal on Selected Areas in Communications, 21(8):1332–1345, 2003.

[XCTT02] G. Xue, L. Chen, K. Thulasiraman, and A. Z. Temp. Delay reduction in redundant trees for preplanned protection against single link/node failure in 2-connected graphs. IEEE Global Telecommunications Conference - GLOBECOM, 13, 2002.

[XXQ02] D. Xu, Y. Xiong. and C. Qiao. Protection with multi-segments (PROMISE) in networks with shared risk link groups (SRLG). In Proceedings of the Annual Allerton Conference on Communication Control and Computing, volume 40, pages 987–996. 2002.

[XXQ03] D. Xu, Y. Xiong. and C. Qiao. Novel algorithms for shared segment protection. IEEE Journal on Selected Areas in Communications, 21(8):1320–1331, October 2003.

[XXQL04] D. Xu. Y. Xiong. C. Qiao. and G. Li. Failure protection in layered networks with shared risk link groups. IEEE network. 18(3):36–41. 2004.

[YADA01] Y. Ye, C. Assi, S. Dixit, and M. A. Ali. A simple dynamic integrated provisioning/protection scheme in IP-over-WDM networks. IEEE Communications Magazine, 39(11):174–182, 2001.

[ZJM00] H. Zang, J. P. Jue, and B. Mukherjee. A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks. Optical Networks Magazine, 1(1):47–60, 2000.

[Zus] Zuse-Institute Berlin (ZIB). http://sndlib.zib.de/home.action.

[ZY02a] H. Zhang and O. Yang. Finding protection cycles in DWDM networks. In IEEE International Conference on Communications (ICC 2002), volume 5, pages 2756–2760, 2002.

[ZY02b] Y. Zhang and OWW Yang. A distributed tree algorithms for WDM network protection/restoration. High Speed Networks and Multimedia Communications 5th IEEE International Conference on. pages 289–294, 2002.

[ZZB05] Z. Zhang, W Zhong, and S. B. Bose. Dynamically survivable WDM network design with p-cycle-based PWCE. IEEE Communications Letters, 9(8):756–758, August 2005.