

# **Extending OWns to Include Protection Functionality**

by

**Albert-Bruce Chittenden**

Submitted in partial fulfillment of the requirements for the degree

**Master of Engineering (Electronic Engineering)**

in the

Faculty of Engineering, Built Environment

and Information Technology

University of Pretoria, Pretoria

November 2005

Die uitbreiding van OWns om beskermingsvaardighede in te sluit  
deur  
Albert-Bruce Chittenden

Promotor: Prof. F. W. Leuschner

Departement: Elektriese, Elektroniese en Rekenaar-Ingenieurswese

Graad: Magister in Elektroniese Ingenieurswese

## Opsomming

Die doel van hierdie verhandeling is om die vermoë van 'n bestaande simulasië-pakket wat gebruik word om vesel-optiese netwerke te simuleer, uit te brei. Sekere van hierdie verbeteringe sluit die vermoë in om 'n beskermingsmeganisme na skakelfaling toe te pas, wat noodsaaklik is in regte-wêreld optiese netwerke om die vloei van verkeer toe te laat na 'n faling in een of meer van die skakels in die netwerk. Nog 'n bydrae is die vermoë van die sagteware om addisionele moontlike roetes vir netwerkverkeer toe te laat. Hierdie verbeteringe sowel as die oorspronklike simulasië sagteware is opebron: dit laat enige persoon toe om die bronkode te verander om sy of haar behoeftes te pas.

Hierdie verhandeling fokus op net-gebaseerde optiese netwerk topologieë, wat gereedelik gevind word in wye-area optiese ruggraatnetwerke, maar wat ook toenemend gevind word in metropolitaanse netwerke. Die wye-area netwerke maak almal gebruik van golflengte-verdelingsmultiplexering ("WDM"), waar verskillende golflengtes van lig op dieselfde fisiese vesel-optiese kabel geplaas word. Die faling van 'n enkele optiese vesel sal dus die faling van verskeie vesel-optiese konneksies tot gevolg hê.

'n Vesel-optiese netwerkontwerper moet verskeie teenstrydige vereistes in ag neem wanneer hy of sy 'n netwerk ontwerp: dit moet huidige en voorspelde toekomstige verkeersvolumes kan hanteer, dit moet bestand wees teen die faling van toerusting, en dit moet so goedkoop as moontlik wees. Die netwerkontwerper moet dus die vermoë besit om verskeie netwerk-topologieë en -scenarios te simuleer: 'n goeie netwerksimuleerder sal waardevolle hulp verskaf om 'n optimale oplossing te vind.

Beskerming en herstelling moet beskou word saam met roeterings- en golflengtetoeëkenning (“RWA”), om te verseker dat alle hulpbronne in die netwerk ten volle benut word. Daar sal ook gekyk word na ’n konneksie se herstellingstyd: dit moet so kort as moontlik wees om netwerk-aftyd en gevolglike verlies aan inkomste te minimeer. Die gekose alternatiewe roete moet ook so kort as moontlik wees om die gebruik van hulpbronne te minimeer en dus die vermoë om verkeer te dra te maksimeer. Die blokkeringswaarskynlikheid, oftewel die onvermoë om ’n konneksie op te stel as gevolg van ’n oorlaaide netwerk, is ’n kritieke faktor en word ook in diepte ondersoek.

Die topologieë wat in hierdie verhandeling ondersoek word, bestaan uit regte-wêreld wye-area WDM vesel-optiese netwerke. Die impak van verskeie enkel sowel as veelvuldige skakelfalings, die toeëkenning van addisionele roetes, sowel as die impak van ’n beskermingsmeganisme, word ondersoek.

Die beoogde doelwitte van hierdie verhandeling is behaal. Die vermoë om enkel sowel as veelvuldige skakelfalings te simuleer is bygedra tot die simulasiepakket. Die blokkeringswaarskynlikhede van verskillende topologieë is vergelyk met mekaar in die teenwoordigheid van skakelfalings. Daar is ook sukses behaal met die implementasie van ’n derde alternatiewe roete in die sagtewarepakket.

## **Sleutelwoorde**

golflengte-verdelings multipleksering; verbindingsfaling; veelvoudige verbindingsfaling; verbindingskoste; nodusfaling; beskerming; herstelling; net-topologie; roeterings- en golflengtetoeëkenning; blokkeringswaarskynlikheid; simulasië sagteware; oopbronnkode; programmatuur

The extension of OWns to include protection functionality

by

Albert-Bruce Chittenden

Promotor: Prof. F.W. Leuschner

Department: Electrical, Electronic and Computer Engineering

Degree: Master of Electronic Engineering

## Summary

The objective of this dissertation is to enhance the functionality of an existing simulation package that is used to simulate fiber optic networks. These enhancements include the capability to simulate protection mechanisms following link failure, which is a necessity in real-world optical networks to ensure the continued flow of information following a failure in a part of the network. The capability for network traffic to choose from additional paths is also an addition to the software. The enhanced, as well as the original simulation software, are open source: this allows anyone to freely modify and improve the source code to suit his or her requirements.

This dissertation will focus on mesh-based optical network topologies, which are commonly found in regional optical backbone networks, but which are also increasingly found in metropolitan areas. The regional networks all make use of wavelength division multiplexing (WDM), which consists of putting multiple different wavelengths of light on the same physical fiber. A single fiber breakage will therefore disrupt multiple fiber-optic connections.

A fiber-optic network designer has to satisfy various conflicting requirements when designing a network: it must satisfy current and predicted future traffic requirements, it must be immune to equipment failure, but it must also be as inexpensive as possible. The network designer therefore has to evaluate different topologies and scenarios, and a good network simulator will provide invaluable assistance in finding an optimal solution.

Protection and restoration need to be looked at in conjunction with routing and wavelength assignment (RWA), to ensure that resources in a network are used at maximum efficiency. Connection restoration time will also be looked at: this should be minimised to ensure minimal network downtime and ensuing loss of revenue. The chosen alternate connection path should also be as short as possible to minimise use of resources and maximise the carrying capacity of the network. Blocking probability (the inability to establish a connection due to a congested network) is a crucial factor and is also investigated.

The topologies investigated in this dissertation consist of various mesh based real-world regional WDM fiber-optic networks. The impact of various link failures, the addition of additional alternate paths, as well as the effect of a protection mechanism on these topologies are also investigated.

The proposed goals were all successfully achieved. The capability of simulating single as well as multiple link failures was introduced to the simulation package. The blocking probability of various network topologies was compared to each other in the presence of link failures. Success was also achieved in the introduction of a third alternate path to the simulation package.

## **Keywords**

wavelength division multiplexing; link failure; multiple link failure; link cost; node failure; protection; restoration; mesh topology; routing and wavelength assignment; blocking probability; simulation software; open source software

My sincere gratitude and thanks to:

My promotor, Professor F.W. Leuschner, for his guidance and encouragement.

My colleagues in the optical networks group, Ronnelle Geldenhuys and Tondi Mangara, for their ideas and enthusiasm.

My friends and family, for their sustained support, motivation and patience.

## List of abbreviations

3R	Regenerating, Retiming and Reshaping
AAL	ATM Adaptation Layer
ACTS	European Advanced Communications Technology and Services
ADM	Add-Drop Multiplexer
ANSI	American National Standards Institute
AON	All-Optical Network
AOTF	Acousto-Optic Tunable Filter
APD	Avalanche PhotoDiode
APS	Automatic Protection Switching
ASE	Amplified Spontaneous Emission
ATM	Asynchronous Transfer Mode
ATMOS	Asynchronous Transfer Mode Optical Switching
BER	Bit-Error Rate
BH	Buried Heterostructure
BHP	Burst Header Packet
BLSR	Bidirectional Line-Switched Ring
BONeS	Block Oriented Network Simulator
BONRA	Bi-directional Optical Network Restoration Algorithm
BP	Blocking Probability
CBR	Constant Bit Rate
CO	Central Office
CWDM	Coarse WDM
dB	decibel
DBR	Distributed Bragg Reflector
DCS	Digital Cross-connect System
DFA	Doped Fiber Amplifier
DFB	Distributed FeedBack
DFN	Deutsches Forschungsnetz

DMUX	Demultiplexer
DNOS	Distributed Network Operating System
DP	Disjoint Path
DPP	Distributed Pre-Planning
DRA	Distributed Restoration Algorithm
DSL	Digital Subscriber Line
DVB	Digital Video Broadcast
DWDM	Dense WDM
EDFA	Erbium Doped Fiber Amplifier
EON	European Optical Network
EoS	Ethernet over SONET/SDH
ETSI	European Telecommunications Standards Institute
FBG	Fiber Bragg Grating
FC	Fibre Channel
FMU	Fault Monitoring Unit
FPR	Fast Path Restorable
F(R)	Reserved Fiber
F(W)	Working Fiber
GbE	Gigabit Ethernet
Gbps	Gigabits per second
GFP	Generic Framing Procedure
GMPLS	Generalized MPLS
HDTV	High Definition Television
ILP	Integer Linear Program
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LED	Light Emitting Diode
LLR	Least-Loaded Routing
LMP	Link Management Protocol
LOA	Loss of Alignment
LOM	Loss of Multiframe
LP	Linear Programming



LSP	Label Switched Path
LTE	Line-Terminating Equipment
MAC	Medium Access Control
MAN	Metropolitan Area Networks
Mbps	Megabits per second
MCMF	Multi Commodity Maximum Flow
MC-OXC	Multicast Capable OXC
MC-RWA	MultiCast RWA
MEMS	MicroElectroMechanical System
MILP	Mixed Integer Linear Programming
MIP	Mixed Integer Programming
MIRR	Minimum Interference Restorable Routing
MPLS	MultiProtocol Label Switching
MP $\lambda$ S	MultiProtocol Lamda Switching
MS-SPRing	Multiplex-Section Shared-Protection Ring
MUX	Multiplexer
MZI	Mach-Zehnder Interferometer
NEST	Network Simulation Testbed
NAM	Network Animator Module
nm	nanometer
NS	Network Simulator
NS2	Network Simulator 2
NMS	Network Management System
NNI	Network-Node Interface
NWC	Non-Wavelength Continuous
OA	Optical Amplifier
OAM	Operations, Administration and Maintenance
OADM	Optical ADM
OAM&P	Operation, Administration, Maintenance and Provisioning
OBS	Optical Burst Switching
OCS	Optical Cross-connect System
OCS	Optical Circuit Switching
ODP	Optical Data Protection
OEO	Optical to Electrical to Optical
OLR	Optical Layer Restoration

OPS	Optical Packet Switching
OPXC	Optical Path Cross-Connect
OR	Optical Receiver
OS	Optical Sender
OSC	Optical Supervisory Channel
OSI	Open Systems Interconnect
OSNR	Optical Signal-to-Noise Ratio
OSPF	Open Shortest Path First
OTcl	Object Tool command language
OTDR	Optical Time-Domain Reflectometer
OTN	Optical Transport Network
OTU	Optical Translation Unit
OWns	Optical WDM network simulator
OXC	Optical Cross Connect
PBT	Polybutylene Terephthalate
PDU	Protocol Data Unit
PE	Polyethylene
PER	Packet Error Rate
PIN	Positive Intrinsic Negative
PI-LOSS	Path Independent LOSS
PMD	Polarisation Mode Dispersion
PNE	Path Number Efficiency
PON	Passive Optical Networking
PoP	Point of Presence
PoS	Point of Service
Post-OA	Optical Post-amplifier
PMD	Polarization Mode Dispersion
Pre-OA	Optical Pre-amplifier
PSR	Path Switched Ring
QoS	Quality of Service
REGEN	REGENERator
RF	Radiofrequency
RIN	Relative Intensity Noise
RLO	Restricted Link Optimization
RPR	Resilient Packet Rings

RSVP-TE	Reservation Protocol with Traffic Engineering
RWA	Routing and Wavelength Assignment
SAFE	South Africa Far East
SAT-3	South Atlantic Telecommunications cable no. 3
SCA	Spare Capacity Allocation
SCM	SubCarrier Multiplexed
SDH	Synchronous Digital Hierarchy
SDL	Switched fiber Delay Lines
SEM	Scanning Electron Microscope
SLA	Service Level Agreement
SLE	Static Lightpath Establishment
SLOB	Switch with Large Optical Buffers
SMOP	Shared-Memory Optical Packet
SOA	Semiconductor Optical Amplifier
SONET	Synchronous Optical NETWORK
SNR	Signal-to-Noise Ratio
SQM	Loss of Sequence
SRLG	Shared Risk Link Group
Tbps	Terabits per second
Tcl	Tool command language
TCP	Transmission Control Protocol
THz	Terahertz
TDM	Time Division Multiplexing
TWA	Traveling Wave Amplifier
UDP	User Datagram Protocol
ULO	Unrestricted Link Optimization
UNI	User-Network Interface
UPSR	Unidirectional Path-Switched Ring
UTP	Universal Transport Protocol
VC	Virtual Concatenation
VCAT	Virtual ConCATenation
VCG	Virtual Concatenation Group
VCSEL	Vertical-Cavity Surface-Emitting Laser
VINT	Virtual InterNet Testbench
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network
VPON	Virtual Private Optical Network
VWP	Virtual Wavelength Path
WAN	Wide Area Network
WASC	West African Submarine Cable
WDM	Wavelength Division Multiplexing
WDMUX	Wavelength De-Multiplexer
WIXC	Wavelength Interchanging Cross-Connect
WMUX	Wavelength Multiplexer
WP	Wavelength Path
WSXC	Wavelength Selective Cross-Connect
ZHLS	Zero Halogen Low Smoke
lamda(R)	Reserved Wavelength
lamda(W)	Working Wavelength

## Contents

Opsomming .....	i
Summary.....	iii
List of abbreviations .....	vi
<b>1 Introduction</b> .....	<b>1</b>
1.1 Background.....	1
1.2 Motivation .....	5
1.3 Objectives .....	6
1.4 Contribution.....	7
1.5 Overview .....	7
<b>2 An overview of optical technology</b> .....	<b>9</b>
2.1 Introduction .....	9
2.1.1 Optical fiber.....	9
2.1.2 Optical sources .....	11
2.1.3 Optical detectors.....	13
2.1.4 Optical amplifiers .....	14
2.1.5 Wavelength switching components.....	16
2.2 SONET / SDH .....	21
2.3 Various networking protocols .....	22
2.3.1 ATM .....	22
2.3.2 MPLS and MPλS .....	23
2.4 The future of optical systems.....	24
<b>3 Optical network topologies</b> .....	<b>27</b>
3.1 Introduction .....	27
3.2 Network topologies.....	28
3.2.1 1 + 1 DP networks .....	28
3.2.2 The path-switched ring .....	29
3.2.3 The mesh topology .....	31
3.2.4 Special topologies.....	36

<b>4</b>	<b>Protection and restoration</b>	<b>38</b>
4.1	Introduction .....	38
4.2	SONET / SDH and the OSI protocol stack.....	39
4.3	Routing and wavelength assignment .....	42
4.3.1	Routing .....	43
4.3.2	Wavelength assignment.....	45
4.4	Protection and restoration.....	46
4.4.1	Protection in 1 + 1 DP and path-switched ring networks.....	46
4.4.2	Protection and restoration in mesh-based optical network topologies .....	48
4.5	Centralised vs de-centralised (distributed) .....	52
<b>5</b>	<b>Network simulator packages</b>	<b>56</b>
5.1	Available network simulator packages.....	56
5.2	Network simulator 2 .....	59
5.3	OWns .....	64
<b>6</b>	<b>Design methodology</b>	<b>69</b>
6.1	Chosen network topologies .....	69
6.1.1	The United States backbone network.....	69
6.1.2	The Italian backbone network .....	71
6.1.3	The DFN network.....	72
6.2	Representation of data in NS2 and OWns .....	74
6.2.1	Graphical representation of network events and traffic .....	74
6.2.2	Limitations of OWns (excluding restoration and protection).....	77
6.2.3	Tcl file breakdown of OWns .....	78
6.3	Design methodology .....	78
6.4	Scope of this work .....	81
6.4.1	Improvements made to OWns .....	81
6.4.1.1	Introduction of random link failures.....	81
6.4.1.2	Introduction of a third path.....	84
6.4.1.3	Introduction of a protection scheme to OWns.....	85
6.4.2	Description of simulation scenarios .....	88

<b>7</b>	<b>Results</b>	<b>92</b>
7.1	Blocking probability .....	92
7.2	Path usage .....	103
7.3	Link utilization .....	107
<b>8</b>	<b>Conclusion</b>	<b>109</b>
8.1	Summary	109
8.2	Assessment	109
8.3	Future work	111
	<b>References</b>	<b>112</b>
	<b>Appendix A – Complete simulation results</b>	<b>121</b>
	<b>Appendix B – List of figures</b>	<b>130</b>
	<b>Appendix C – List of tables</b>	<b>134</b>

# Chapter 1

## Introduction

### 1.1 Background

Fiber optic communication networks have emerged in the last two decades to become the technology of choice for the transport of large volumes of voice as well as data information over large distances [1]. Copper wires simply lack the necessary bandwidth capability and radio networks have finite bandwidth, while satellite communications suffer from delays that make real-time communication problematic. Constant improvements in technology allow fiber optic networks to put more and more wavelengths of light on to the same physical fiber, which make fiber optic networks the ideal choice to deal with future traffic demands.

The human eye can detect wavelengths from approximately 400 to 700 nanometer (nm). Long distance fiber optic systems typically utilise light in the infrared region with a wavelength of around 1500 nm, due to the low attenuation of optical fibers in this wavelength range. In just the 1500 nm band the usable bandwidth of one single-mode fiber is approximately 25 000 GHz, which is 1000 times the entire usable radio frequency spectrum (taking into account that the Earth's oxygen absorption attenuates RF at higher frequencies) [2].

In recent years there has been a remarkable growth in the volume of data transmitted through the core optical communication networks of telecommunication providers. This has been prompted by various factors, including rising population numbers, an increasing percentage of citizens worldwide that have access to telecommunication services, and the



explosive growth of the Internet. The explosive growth of cellular telephony in developing countries also demands bandwidth from fiber optic networks. New innovative services such as video on demand, high definition television (HDTV) and video-conferencing, as well as new business practices such as telecommuting in developed countries promise to increase the worldwide demand for bandwidth even further [3]. This has prompted telecommunication companies to implement wavelength division multiplexing (WDM), utilising more and more wavelengths per optical fiber to accommodate rising traffic volumes [4].

WDM can be broadly grouped into two groups: dense wavelength division multiplexing (DWDM), and coarse wavelength division multiplexing (CWDM). The International Telecommunications Union (ITU) issues standards to ensure that the equipment from various manufacturers will perform reliably in any network. DWDM (ITU-T standard G.694.1) [5] is mostly used where there is a need to concentrate a very heavy load of traffic onto a fiber: it is typically used in developed countries on regional links between large cities, thus making up the backbone of these networks. Due to the need to multiplex numerous non-overlapping wavelengths onto one fiber, all optical components in the system (lasers, receivers, add-drop multiplexers (ADMs) and fiber-bragg gratings etc.) need to be of a high standard and conform to strict specifications.

Table 1.1: DWDM (ITU-T G. 694.1) frequency spacing grid [5].

Nominal central frequencies (THz) for spacings of				Approximate nominal central wavelengths (nm)
12.5 GHz	25 GHz	50 GHz	100 GHz and above	
195.9375	-	-	-	1530.04
195.9250	195.925	-	-	1530.14
195.9125	-	-	-	1530.24
195.9000	195.900	195.90	195.9	1530.33
195.8875	-	-	-	1530.43
195.8750	195.875	-	-	1530.53
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
193.1250	193.125	-	-	1552.32
193.1225	-	-	-	1552.42
193.1000	193.100	193.10	193.1	1552.52
193.0875	-	-	-	1552.62
193.0750	193.075	-	-	1552.73
193.0625	-	-	-	1552.83
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
184.5625	-	-	-	1624.34
184.5500	184.550	184.55	-	1624.45
184.5375	-	-	-	1624.56
184.5250	184.525	-	-	1624.67
184.5125	-	-	-	1624.78
184.5000	184.500	184.50	184.5	1624.89

CWDM systems (ITU-T standard G.694.2) [6], on the other hand, is a relatively new specification that is generally used on links where there is considerable traffic, but not enough to warrant an expensive DWDM setup. Typical uses include links between major cities in developing countries, links between smaller cities in developed countries, and metropolitan area networks (MANs). Due to the increased spacing between wavelengths CWDM systems utilise lasers, receivers and ADMs that can have more relaxed specifications than the components used in DWDM systems. This leads to considerable cost savings.

Table 1.2: CWDM (ITU-T G. 694.2) wavelength spacing grid [6].

<b>Nominal central wavelengths (nm) for CWDM spacing of 20 nm</b>
1271
1291
1311
1331
1351
1371
1391
1411
1431
1451
1471
1491
1511
1531
1551
1571
1591
1611

Wavelength  $\lambda$  and frequency  $f$  are related by the formula

$$c = \lambda * f \quad (1.1)$$

where  $c$  is  $2.99793 \times 10^8$  meter per second,  $\lambda$  is measured in meter and  $f$  is measured in Hertz.

The question might be asked whether it would not be easier to lay more fiber, instead of utilising WDM. The answer lies in the prohibitive cost of deploying more fiber, especially on longer links. The fiber itself is relatively inexpensive, but the cost of installing fiber in underground trenches and the required person-hours is very expensive. It is a lot quicker and cheaper to go the WDM route: install more lasers, receivers and ADMs while utilising the same fiber. WDM is thus a cost-effective solution, but in the event of a fiber fault all the traffic on all the wavelengths utilised on that specific fiber are lost.

Typical causes of fiber faults include theft, construction activities, earthquakes and severe weather [7].

At a typical data rate of 10 Gbps per wavelength, and up to 160 wavelengths per DWDM fiber or up to 18 wavelengths per CWDM fiber, this results in significant loss of revenues to the service provider [8]. This necessitates the use of protection and restoration in fiber optic networks.

## 1.2 Motivation

The failure of parts of a fiber optic network is inevitable: not only due to equipment failure but also due to external factors beyond the control of the network designer, e.g. earthquakes or vandalism. This forces the designer to design a network that is robust in nature: this means that the network can survive certain failures with minimal impact to the customer.

It is intuitive to notice that the more routes between two points in a network, the higher the redundancy of the network will be. Unfortunately, a network cannot only be designed according to technical considerations: financial restraints are also in place which must be adhered to. The network designer therefore has to find the optimal point between redundancy and cost, which will satisfy both the end-user as well as the investors who financed the project.

The network simulation package is a crucial part of the network designer's armament: it allows him or her to simulate different network topologies with different levels of redundancy. It also allows different routing and wavelength assignment (RWA) algorithms to be implemented and tested. Random or specific link failures can be implemented to ascertain the adverse effect it has on the network.

It is therefore crucial that the network designer has access to a fiber optic network simulator that has all the needed capabilities to implement an efficient network.

Protection involves setting up alternate routes during connection setup, while restoration determines new routes after a link failure. Many different algorithms exist, which give different results with regards to restoration time, blocking probability, network scalability etc.

When designing a network with regard to operation, protection and restoration aspects, it is essential to compare the results of various algorithms with suitable simulation software to determine which algorithm is most suitable.

### **1.3 Objectives**

The objective of this dissertation is to simulate and compare the performance of protection algorithms in various mesh-based optical WDM networks with regards to:

- blocking probability,
- path usage,
- restoration time.

Another factor that will also receive close attention is the effect that different connectivity factors will have on the network topologies selected for simulation.

## 1.4 Contribution

The chosen open-source fiber optic network simulator, OWns, is incapable of simulating single- or multiple-link failure in fiber optic networks. Therefore, it is incapable of performing protection or restoration. In addition to the above, it is also limited in its default RWA algorithms.

This dissertation will therefore implement an extension to OWns that will allow the package to perform protection when faced with one or more link failures.

After an extensive literature study, no mention was found of any individual or corporation that investigated the field of optical WDM restoration and protection by using OWns. By extending the OWns capabilities to include restoration and protection capabilities, the network designer is capable of testing and comparing the performance of different algorithms with respect to different network topologies.

In short, this dissertation will strive to implement OWns in the optimisation of restoration and protection algorithms in optical fiber network planning.

## 1.5 Overview

In chapter 2, the reader will find an overview of all components that are needed for a modern fiber optic network to function. The most used protocols and standards for optical networks are also mentioned and briefly explained. A short section is dedicated to a possible future look of optical networks.

Chapter 3 focuses on the different optical network topologies that can be found today. Some of the topologies mentioned include the 1+1 disjoint path, ring and mesh networks, as well as networks that do not fit into one of the above-mentioned categories. Network layouts for some real-world wide area optical networks are given as well.

Protection and restoration are discussed in considerable detail in chapter 4. All the factors that are relevant are discussed, including protocol stacks, routing and wavelength assignment, differences between protection and restoration, centralised and distributed algorithms etc.

Chapter 5 discusses the available network simulator packages available today. Reasons are given for the choice of NS2 over other alternatives, as well as some code illustrating the functionality of the software. The functioning of the optical add-on package, OWns, is also explained in detail.

In chapter 6, the reader can find the design methodology. The chapter starts off with the real-world network topologies that will be simulated. Screen shots are shown in which the reader can see the output obtained with NS2 and the base version of OWns. In the next sections, the reader is taken through the steps which were taken to achieve the desired added functionality to OWns, namely adding protection capabilities to the software. Next, the parameters for all the different simulation scenarios are given.

Chapter 7 contains selected results which are given in tabular as well as graphical form. An analysis of the results are also given. The complete results are given in tabular form in Appendix A.

This work concludes with chapter 8, in which the results obtained in chapter 7 are analysed and interpreted. Recommendations for possible future work are given as well.

## Chapter 2

# An overview of optical technology

### 2.1 Introduction

This chapter will give a brief overview of the basic components that are required for a fiber optic network to function. Components covered include optical sources, optical detectors, optical amplifiers, wavelength switching components and the physical optical fiber itself. Coverage will focus on equipment that is currently in use in WDM systems worldwide.

#### 2.1.1 Optical fiber

The optical fiber found in modern day WDM networks typically consists of a silica ( $\text{SiO}_2$ ) core, and a  $\text{B}_2\text{O}_3$ - $\text{SiO}_2$  cladding [9]. The core has a diameter of approximately  $10\ \mu\text{m}$ , and is thus a single-mode fiber. Plastic multi-mode fiber (diameter of  $50$  to  $62.5\ \mu\text{m}$ ), while inexpensive, suffers from attenuation that makes it unsuitable for long distances, and is generally only used in local area networks (LANs). The core and the cladding are the two components that make up the optical fiber itself.

However, the optical fiber, while being able to handle bending forces fairly well, easily fractures when a tensile force is applied. The fiber is also sensitive to impact forces that might break or chip it. To counteract this, a steel or Kevlar tensile strength member is usually added to the fiber optic strands, and everything is enclosed in an outer covering of water-resistant plastic to form a cable. A layer of steel tape is also normally put around the bundles of fiber optic strands to give added protection against burrowing rodents and



construction machinery. It is customary to put multiple fiber optic strands in one fiber optic cable. Refer to figure 2.1 for a typical example of a fiber optic cable.

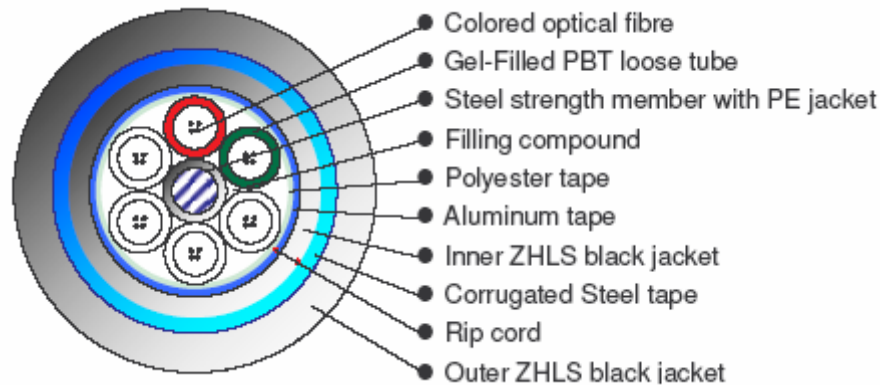


Figure 2.1: Profile of a typical multi-strand fiber optic cable, designed for underground use [10].

Optical fiber attenuation is an important aspect of fiber optic systems, as this directly influences the distance limit of a fiber optic system. It is measured in decibel per kilometer (dB/km). With modern day optical fiber, an attenuation figure of 0.1 dB/km is possible. However, it is important to note that the attenuation figure is not constant across the wavelength range. Traditionally, attenuation has been lowest in the O-band (1260 -1360 nm, centered around 1310 nm) and the C-band (1530 - 1565 nm, centered around 1550 nm). Therefore, fiber optic systems have generally been designed for use in these two regions.

In recent years, optical fiber manufacturers have been able to greatly reduce the water attenuation peak located at 1383 nm. This has opened up the E-band (1360 – 1460 nm) to be used by CWDM applications.

Figure 2.2 shows the 18 standardised CWDM wavelengths (ITU-T 694.2). The DWDM wavelengths (ITU-T 694.1) are located in the C-band, where attenuation is lowest.

There are different fiber types, which are optimised with regard to their intended range of operation. Non-dispersion shifted fiber should conform to ITU-T G.652, and is optimised for 1310 nm. Non-zero dispersion-shifted fiber conforms to ITU-T G.655 and is optimised

for the 1550 nm transmission region, where DWDM transmissions take place. This new standard puts strict limits on the optical fiber's coefficient of polarisation mode dispersion (PMD), and is measured in picoseconds per kilometre<sup>1/2</sup> (ps/ $\sqrt{\text{km}}$ ). PMD is the main limiting factor for high-speed, long-distance communication in single-mode fiber systems.

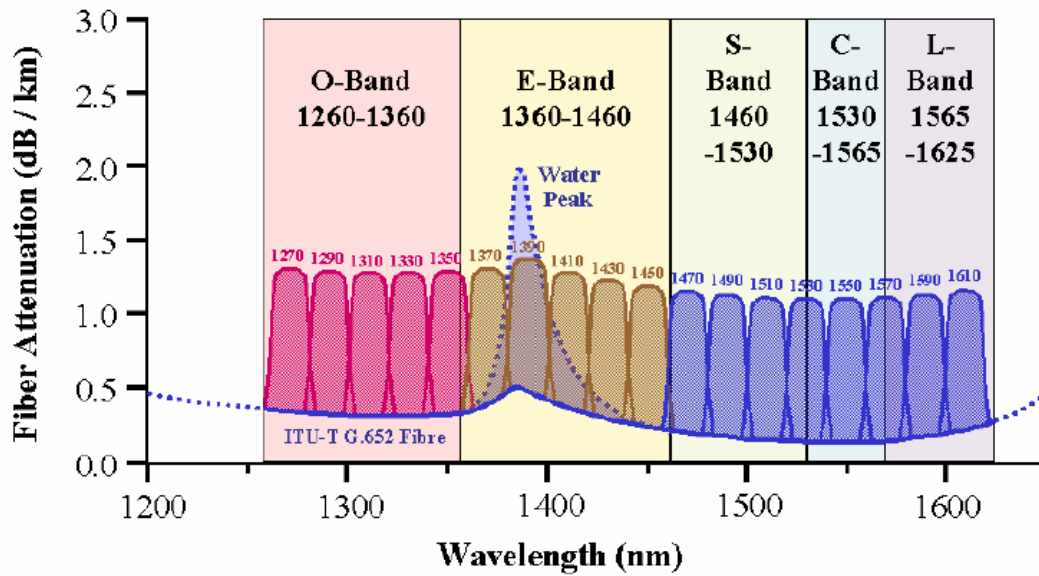


Figure 2.2: Graph of fiber attenuation versus wavelength, showing historic water peak located at 1383 nm. The 18 CWDM wavelengths are also shown [11].

### 2.1.2 Optical sources

Every fiber optic system needs a light source at the transmitting end. There are mainly two different types of optical sources in use, namely light emitting diodes (LEDs) and laser diodes (LDs). Laser diodes, compared to LEDs, have faster response times, narrower spectral bandwidths and much higher directional light output. LEDs are therefore only used in low-speed LAN systems (100 – 200 Mb/s) and laser diodes are used in WDM systems.

The semiconductor laser diode is the laser type of choice for fiber optic networks. There are many different types and configurations: some of these include the Fabry-Perot,

distributed feedback (DFB), buried heterostructure (BH), vertical-cavity surface-emitting laser (VCSEL), distributed-Bragg-reflector (DBR) and many others [9].

The laser can either be modulated internally or modulated externally to produce the modulated data stream. Internal modulation is done by varying the input current to the laser diode, while external modulators modulate the constant output light produced by the laser via an external lens or shutter. The output wavelength of a laser can either be fixed or variable.

Lasers used in DWDM systems need a thermoelectric cooler to keep the laser at a certain temperature: any changes in ambient temperature will cause the output wavelength of the laser to change. This would be unacceptable in DWDM systems where designated wavelength slots are located 0.1 nm (12.5 GHz) apart. In CWDM systems, lasers can generally be left uncooled due to the generous 20 nm channel spacings [11].

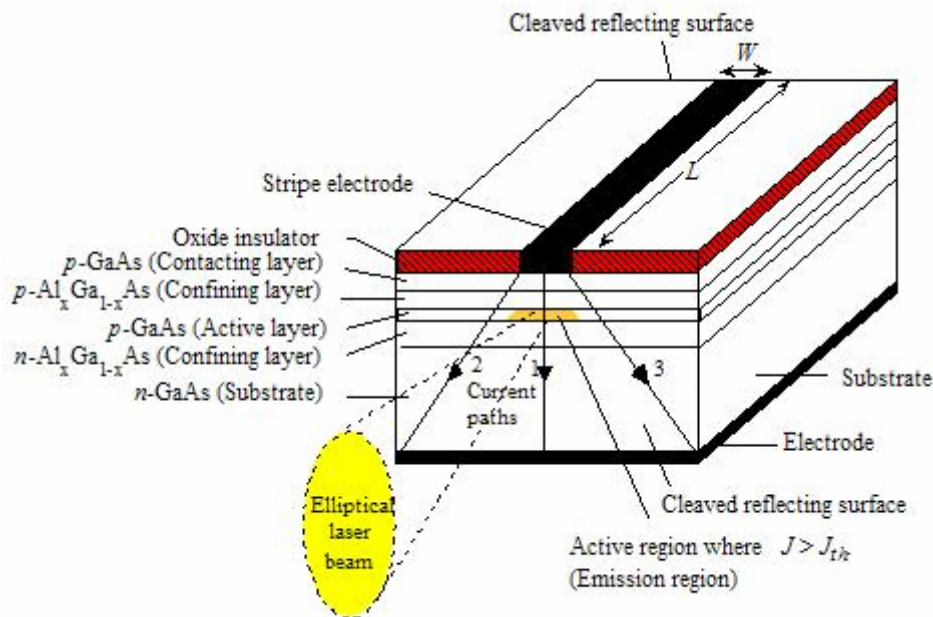


Figure 2.3: Schematic illustration of the structure of a double heterojunction stripe contact laser diode [12].

### 2.1.3 Optical detectors

The two main types of optical detectors in use are the PIN photodiode and the avalanche photodiode (APD). The PIN photodiode gets its name from its physical construction: it consists of a p-type doped region and an n-type doped region, which are separated by a very lightly doped n-doped intrinsic (i) region. The advantages of PIN photodiodes include lower cost and reduced complexity of the receiver design.

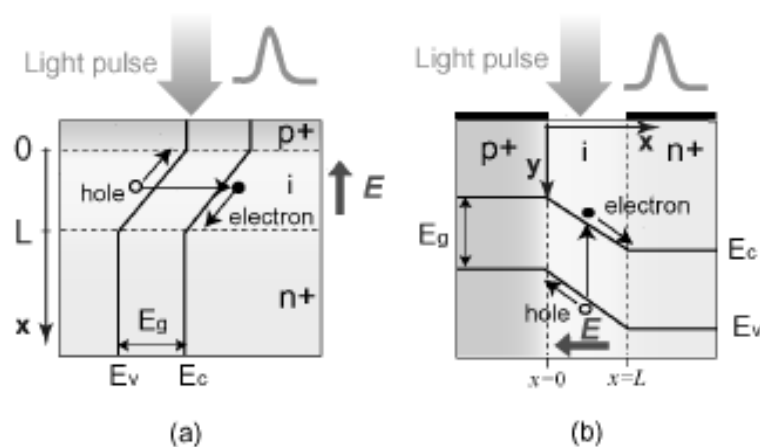


Figure 2.4: Structures of (a) vertical p-i-n photodiode and (b) a lateral p-i-n photodiode [13].

The APD is a modified version of the PIN photodiode: it differs by having an extra p-doped field to create a high electric field strength that creates an avalanche multiplication effect. The advantage is an extra 9-10dB receiver sensitivity [9], however, this comes at increased cost.

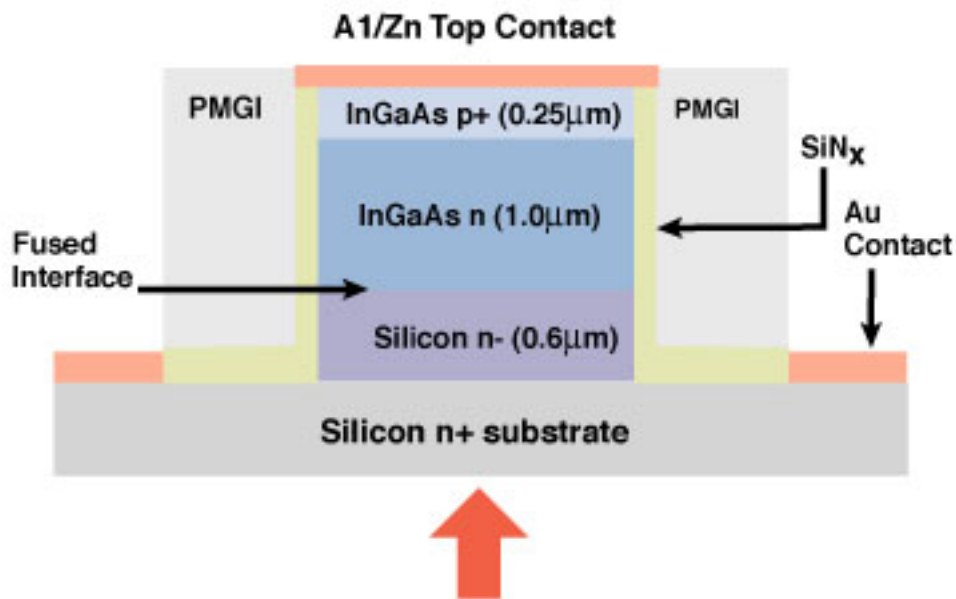


Figure 2.5: Schematic of avalanche photodiode (APD) [13].

The network designer will choose between the two optical detector types after a comprehensive link-budget analysis has been done, to see whether the extra sensitivity offered by the APD is needed or not.

#### 2.1.4 Optical amplifiers

In a typical WDM system, where the transmitter and the receiver may be hundreds of kilometers apart, it is vital to have components in place that can amplify the optical data signal. This is due to the attenuation of the fiber itself, as well as losses brought about by fiber optic splices. The two current technologies in use for optical amplifiers are semiconductor optical amplifiers (SOAs) and doped-fiber amplifiers (DFAs).

The major type of SOA that is in use today is the non-resonant traveling wave amplifier (TWA). The TWA is similar in nature to the semiconductor laser diode, except that lasing does not take place. This means that incoming photons, and thus power levels, can be

increased, but that it cannot generate a coherent output signal by itself. The gain of the TWA comes about from the pumping process that is powered via external current injection.

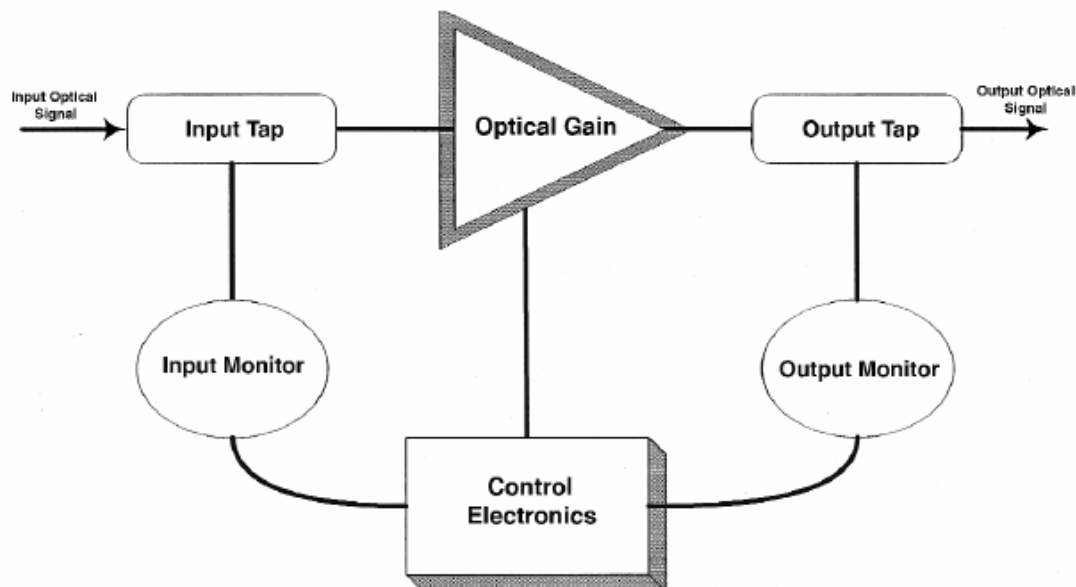


Figure 2.6: Block diagram showing a typical inline amplifier configuration [14].

The DFA typically consists of a piece of fiber-optic fiber, normally between 10 and 30 meters in length, lightly doped with a rare-earth element, such as erbium (Er), neodymium (Nd) or praseodymium (Pr). However, erbium is the element most commonly used, so the erbium doped-fiber amplifier (EDFA) is the DFA most commonly encountered. The two ends of the EDFA are spliced between two lengths of normal fiber optic strands.

The EDFA uses optical pumping to increase optical power levels in the data-carrying wavelengths. A so-called pump wavelength, typically 980nm or 1480nm, is introduced into the fiber-optic strand. When the EDFA-section of the fiber-optic strand is encountered, the interaction between the photons of the pump wavelength, the photons of the data-carrying wavelengths and the erbium atoms cause stimulated emission of photons of the data-carrying wavelengths to take place, and thus the optical power of the data-carrying wavelengths are increased. Monitoring and feedback loops are also used in the typical

EDFA setup to ensure that the outgoing wavelengths of light are at optimum power levels. Please refer to figure 2.7 for a block diagram of a typical EDFA system.

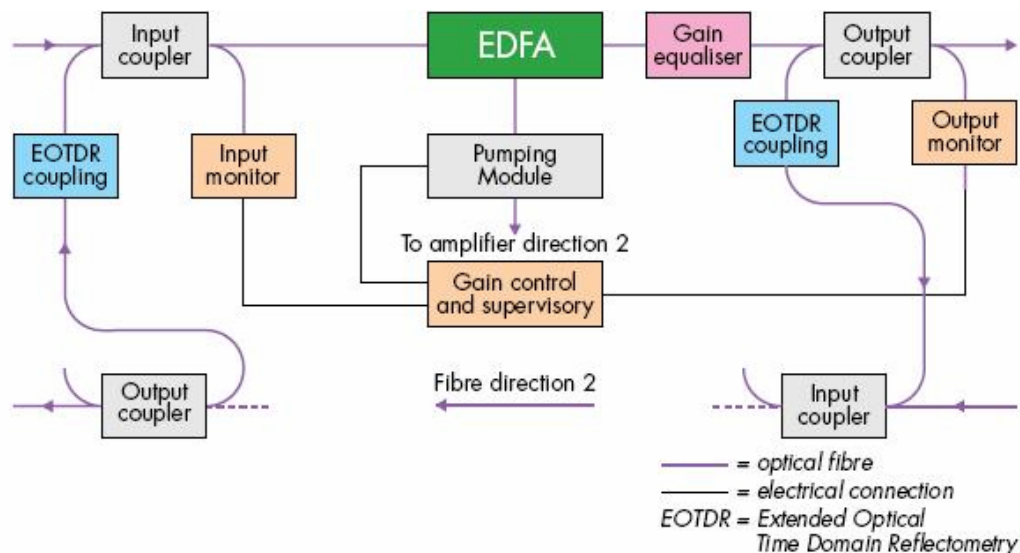


Figure 2.7: Block diagram of EDFA amplification system [15].

The stimulated emission mechanism of the EDFA only takes place with wavelengths of between 1530nm and 1560nm, which coincides with the attenuation minimum of fiber-optic strands (the C-band, 1530-1565nm). This is the main reason that long distance DWDM fiber-optic communication takes place at these wavelengths: expensive amplification equipment can be situated further apart, with considerable cost savings.

### 2.1.5 Wavelength switching components

In an optical network, especially a WDM network, it is not only sufficient to have optical sources, detectors, amplifiers and the optical fiber itself. At some points in the network, it becomes necessary to add or extract wavelengths from the optical fiber, to split an incoming wavelength into multiple outgoing copies of itself, and to convert an incoming wavelength into an outgoing signal of different wavelength, while carrying the same data.

The most basic optical components are the optical combiner and the optical splitter. The optical combiner of size  $N \times M$ , where  $N$  is the number of inputs and  $M$  is the number of outputs, typically consists of an array of fused tapered couplers, and its purpose is to combine the wavelengths from two or more fibers onto one or more output fibers. A fused tapered coupler is shown in figure 2.8. Two single-mode fibers are fused together by heat and pulled apart, resulting in a device with an input power of  $P_0$ , an output power of  $P_1$  into the first fiber, and an output power of  $P_2$  into the second fiber. The output power ratios can be changed by varying parameter  $l$ .

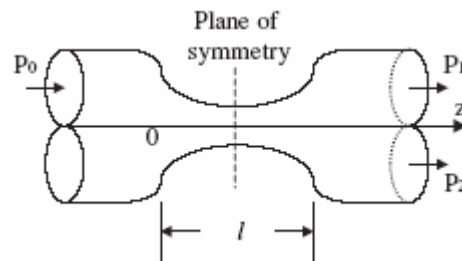


Figure 2.8: Diagram of symmetrical fused tapered coupler [16].

The optical splitter ( $1 : n$ ) is a component that takes a single input data stream of power  $N$ , and splits it onto  $n$  outgoing fibers, each of which has optical power  $1/N$  (for a symmetrical splitter). Splitters of this type are normally used in passive optical networks (PONs), where a service provider provides the same downstream signal to multiple customers.

Gratings are elements which are used for combining (adding) and removal (dropping) of wavelengths in optical systems. The most common type of grating in use is the fiber Bragg grating (FBG). If multiple wavelengths are traveling through an optical fiber containing a repeating periodic structure (grating), the diffractive properties of the periodic structure leads to the reflection of a very narrow wavelength band. The centre wavelength of this narrow wavelength band is represented by the Bragg condition:

$$\lambda_B = 2 \cdot n_{eff} \cdot \Lambda \quad (2.1)$$

where  $\lambda_B$  is the centre wavelength,  $n_{eff}$  is the effective index of the guided mode and  $\Lambda$  is the period of the index modulation.



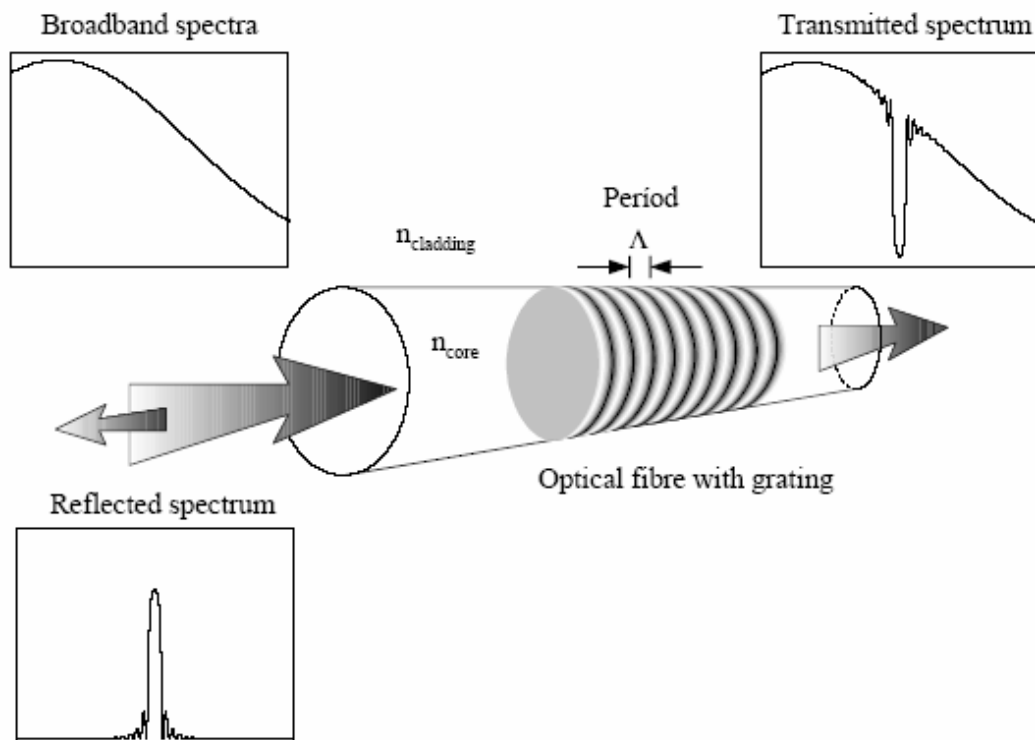


Figure 2.9: Schematic representation of a fiber Bragg grating [17].

The optical add-drop multiplexer (OADM) makes use of both FBGs and fused tapered couplers to fulfill the roles of multiplexers (MUXs) and demultiplexers (DMUXs). The basic OADM consist of a circulator, FBG and a fused tapered coupler. The wavelength that is to be dropped is reflected back by the FBG, and exits at the circulator. The other wavelengths do not satisfy the FBG's criteria, are unaffected by the FBG and passes right through. The wavelength that is to be added enters through the fused tapered coupler onto the optical fiber.

OADMs are used whenever there is a need to add or drop a wavelength to or from a network, this can be at endpoints of the network, or at central switching points. FBGs are generally used when the wavelength that needs to be dropped remains the same. If the wavelength that needs to be dropped changes frequently, a technology that is well suited to change like the acousto-optic tunable filter (AOTF) is generally employed, and has a tuning time in the tens of microseconds range [1].

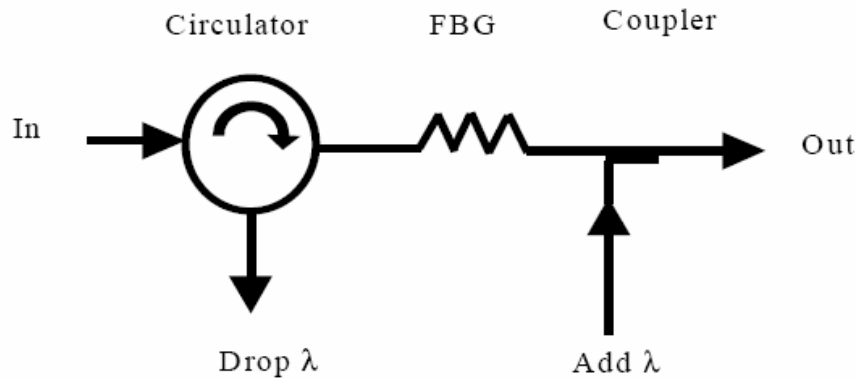


Figure 2.10: Basic OADM architecture, utilising a fiber Bragg grating [17].

The optical cross connect (OXC) is employed when there is the need to route wavelengths from a certain input fiber to a different output fiber. This usually takes place in the central switching offices of the telecommunications service providers. An example of the so-called “crossbar” optical cross connect is shown in figure 2.11. To switch a network consisting of  $N$  inputs and  $M$  outputs,  $N \cdot M$   $2 \times 2$  switches are required. In figure 2.11, we have 4 inputs and 4 outputs. Therefore 16  $2 \times 2$  switches are required. Each of the  $2 \times 2$  switches can have one of two states, either cross or bar. By changing the configuration of all the  $2 \times 2$  switches in the OXC, the input from any fiber can be rerouted to any other fiber. OXCs of  $256 \times 256$  have been constructed [18] (this is  $256^2$  or 65536  $2 \times 2$  switches).

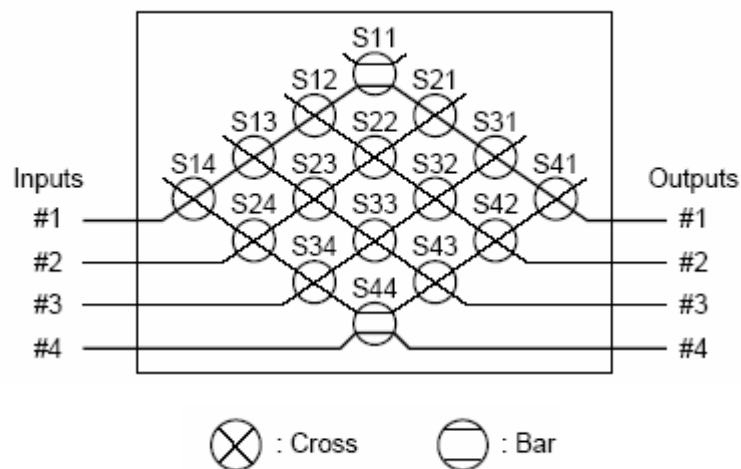


Figure 2.11: Schematic of OXC, utilising  $N^2$  crossbar  $2 \times 2$  switches [19].

Another type of technology that can be found in OXCs is called microelectromechanical systems (MEMS). MEMS consist of miniature mirrors that are etched in silicon, and can be rotated around three dimensions when the correct electrical or magnetic control field is applied. Three dimensional MEMS systems only require  $2 \cdot N$  switches for  $N$  inputs. A schematic for a three-dimensional MEMS OXC system is shown in figure 2.12. A scanning electron microscope picture of a MEMS micro-mirror array is shown in figure 2.12.

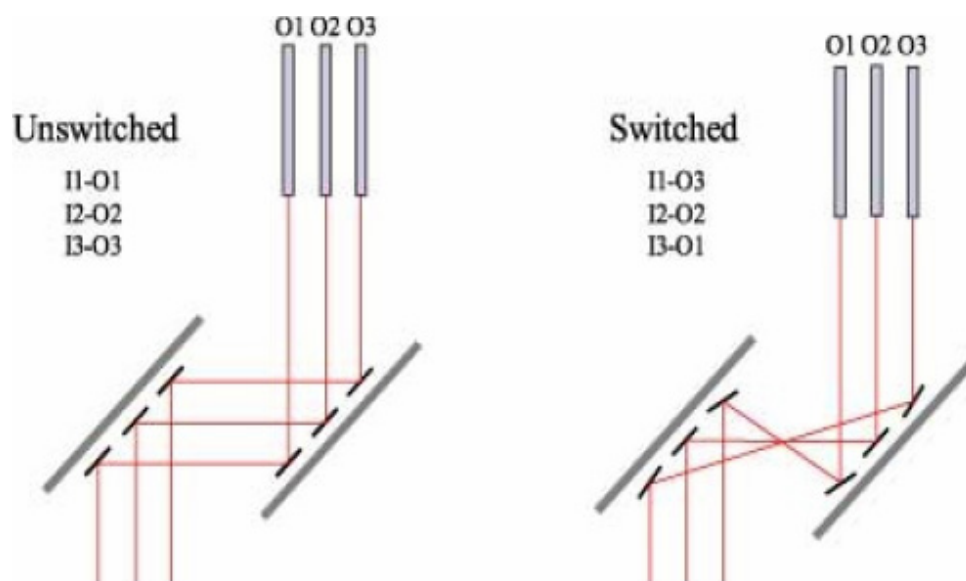


Figure 2.12: 3D MEMS cross-connect in two different states [20].



Figure 2.13: Scanning electron microscope image of MEMS micromirror array [20].

## 2.2 SONET / SDH

In the mid-1980's there was a need to implement a standard that would allow equipment from different manufacturers to be used in the same system. This led to the development of the ANSI T1.105.06 [21] and the ITU-T G.957 [22] standards. The ANSI standard led to the implementation of the synchronous optical network (SONET) and the ITU-T standard led to the implementation of the synchronous digital hierarchy (SDH). SONET is implemented in the United States of America and Japan, while SDH is used in the rest of the world, including South Africa.

Both SONET and SDH make use of time division multiplexing (TDM), and both standards are nearly identical save for some implementation differences. Refer to figure 2.14 for the basic structure of a SONET frame.

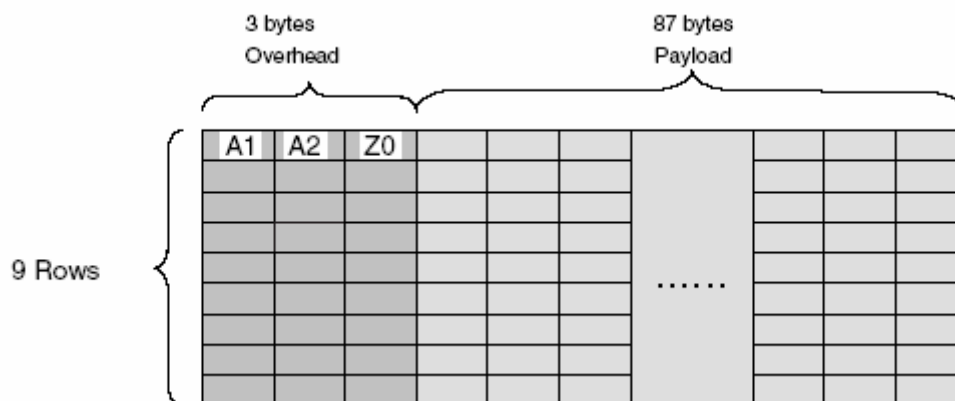


Figure 2.14: Basic SONET STS-1/OC1 (51.84 Mb/s) frame. The first 3 bytes of every frame is used for overhead like signaling [23].

The basic SONET frame is called OC-1 and provides a transmission rate of 51.84 Mb/s [9]. Higher rates can be achieved by using integer multiples, in other words OC- $N$ , where  $N$  is normally 1, 3, 12, 24, 48 or 192. In SDH, the basic transmission rate is called STM-1 and has a transmission speed of 155.52 Mb/s. Higher speeds utilise STM- $M$ , where  $M$  can be 4, 8, 16, 32 or 64. Please refer to table 2.1 for a summary of commonly used SONET and SDH transmission rates.

Table 2.1: Commonly used SONET and SDH transmission rates [9].

SONET level	Electrical level	Line rate Gb/s	SDH equivalent
OC-1	STS-1	0.05184	-
OC-3	STS-3	0.15552	STM-1
OC-12	STS-12	0.62208	STM-4
OC-24	STS-24	1.24416	STM-8
OC-48	STS-48	2.48832	STM-16
OC-96	STS-96	4.97664	STM-32
OC-192	STS-192	9.95328	STM-64
OC-768	STS-768	39.81312	STM-256

## 2.3 Various networking protocols

### 2.3.1 ATM

The asynchronous transfer mode (ATM) networking protocol is widely used in industry. The intended use of ATM was to create a protocol that could support both synchronous protocols like SONET and SDH, while also being able to support packet-based network protocols such as internet protocol (IP). ATM makes use of small, fixed size cells, each containing a payload of 48 bytes and a header of 5 bytes, to provide a networking protocol that minimises delay, thus making it ideal for voice over internet protocol (VoIP) networks. ATM also supports multiple quality of service (QoS) levels [24].

ATM is a highly complex protocol, and makes up layer two of the OSI protocol stack (please refer to section 4.2 for a more thorough discussion of the OSI model). Recent increases in transfer speed of optical as well as electronic networks have mitigated ATM's delay advantage. The small cell size, while perfect for voice applications, is not optimal for data transfer applications. The above-mentioned two factors, coupled to its complexity and related cost, has led to the development of protocols like MPLS that might take over from ATM in the future.

ATM also has the capability to multiplex numerous low-bandwidth packet sources onto a synchronous high-bandwidth platform. This ability of ATM to provide efficient grooming, that is connecting numerous low-bandwidth sources to one high-bandwidth link, coupled with its wide user base, will ensure that ATM will be used for some time to come [24].

### **2.3.2 MPLS and MP $\lambda$ S**

The multi protocol label switching (MPLS) networking protocol is a relatively new protocol that combines layers two and three of the OSI model. The combination of layers two and three of the OSI model leads to a protocol that allows the network operator greater freedom with regard to routing, protection, quality of service and congestion management. This ability of enhanced traffic engineering allows for the optimisation of network resources [25].

MPLS uses constraint-based routing; that is, the shortest path between a source-destination pair is used that conforms to the resource constraints of the link. MPLS works by establishing virtual label switched paths (LSPs) between sources and destinations. A multitude of these virtual LSPs can be aggregated onto one physical data stream by an MPLS edge router. These LSPs can be separated from the data stream at intermediary or destination nodes via other edge routers.

A recent extension to the MPLS protocol is called multi protocol lambda switching (MP $\lambda$ S). MP $\lambda$ S is similar to MPLS, with the exception that MP $\lambda$ S is tailored to the delivery of MPLS services over optical networks. Some of these include the fact that with MPLS there can be a virtually limitless amount of LSPs per physical link, while with MP $\lambda$ S there has to be a one-to-one mapping between wavelengths and labels. Another difference is that MPLS uses unidirectional LSPs, while MP $\lambda$ S uses bidirectional optical LSPs [26].

## 2.4 The future of optical networks

The future look of optical networks is a complicated question with no clear cut answers. The optical network of tomorrow will have to support enormous predicted traffic volumes while still supporting the existing legacy low-bandwidth devices of today. One thing that seems certain is the future disappearance of electronic routing processing on packets in high-speed backbone networks: the traffic between nodes in backbone networks will become more and more transparent, or O-O (optical-optical). The traffic between the edge nodes in networks and the backbone nodes are still likely to be mostly electronic, due to the near impossibility of providing a fiber optic connection to every subscriber in the short and the medium term. This means that the connection between two end users is likely to still be non-transparent (opaque) O-E-O (optical-electrical-optical) due to the electronic elements in the path between them.

The ATM protocol is likely to be replaced by MPLS and its optical derivative MP $\lambda$ S in the future, mostly due to the advantages MPLS and MP $\lambda$ S have with regard to switching of large volumes of data traffic.

The SONET / SDH architecture is slated by some to disappear in the future, replaced by a combination of WDM and OXC architecture. Other observers predict that the SONET / SDH architecture is so widely entrenched that the basic SONET / SDH frame structure is still likely to be with us for years and years to come.

IP has become pervasive in the last few years, it is becoming difficult to find advanced consumer products that do not make use of it. This will ensure the survival of IP in the future, albeit in the envisaged IPv6 format instead of the present IPv4 format. One of IP's biggest disadvantages is its inability to provide differentiated quality of service to different customers. Some views even suggest futuristic optical networks only utilising WDM and IP layers: in order for this view to become reality, extensions will have to be made to WDM to include protection and restoration abilities (presently handled by SONET / SDH),

and IP will have to be extended to include vital QoS capabilities (presently handled by ATM).

Future technologies like optical channel switching (OCS), optical burst switching (OBS) and optical packet switching (OPS) are likely to replace electronic processing of optical packets to a large extent, however these technologies are still many years away from making it to the market.

In short, there are many different opinions on how the optical network of tomorrow will look. Shown in figures 2.15 and 2.16 are two different views on the layered architecture of tomorrow's optical networks. The authors agree on the presence of WDM and IP, but disagree on the other elements that will make up the optical networks of tomorrow.

In figure 2.17, a possible view of a complete future telecommunications network is given. Elements shown include the home network, the access network, the metropolitan area network and the long-haul backbone network.

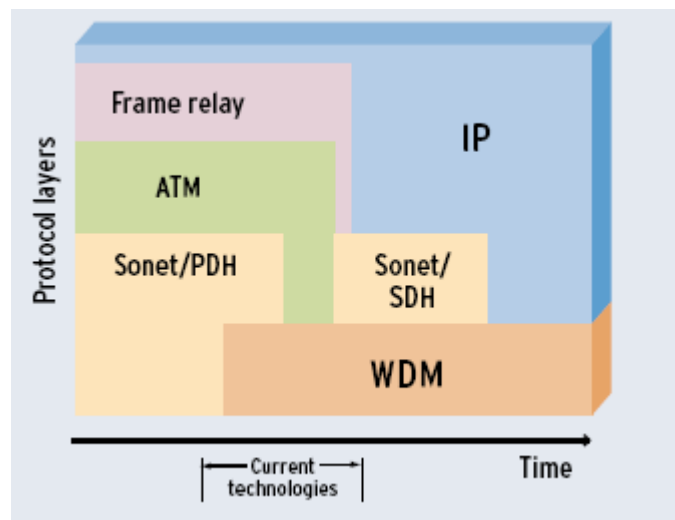


Figure 2.15: Possible evolution of optical protocol stack over time [27].



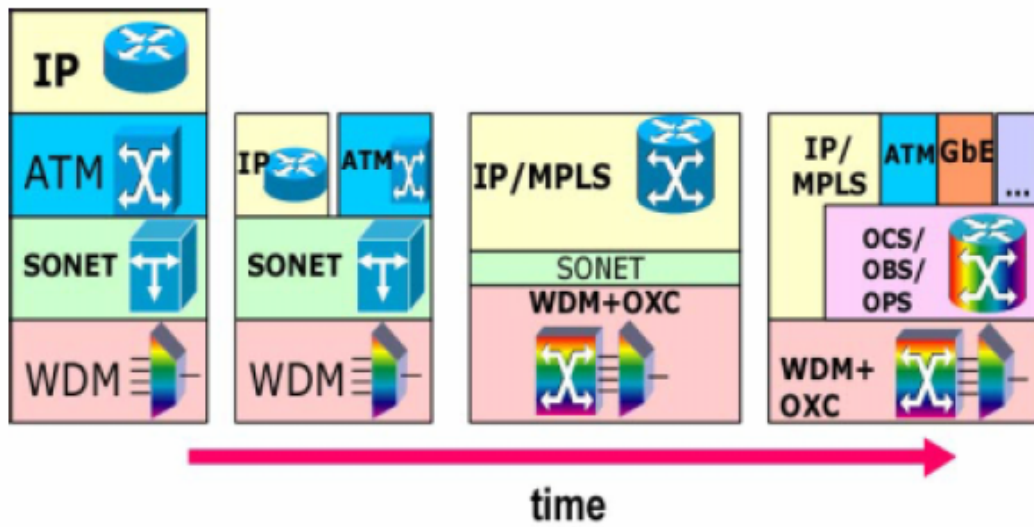


Figure 2.16: Possible evolution of optical protocol stack over time [28].

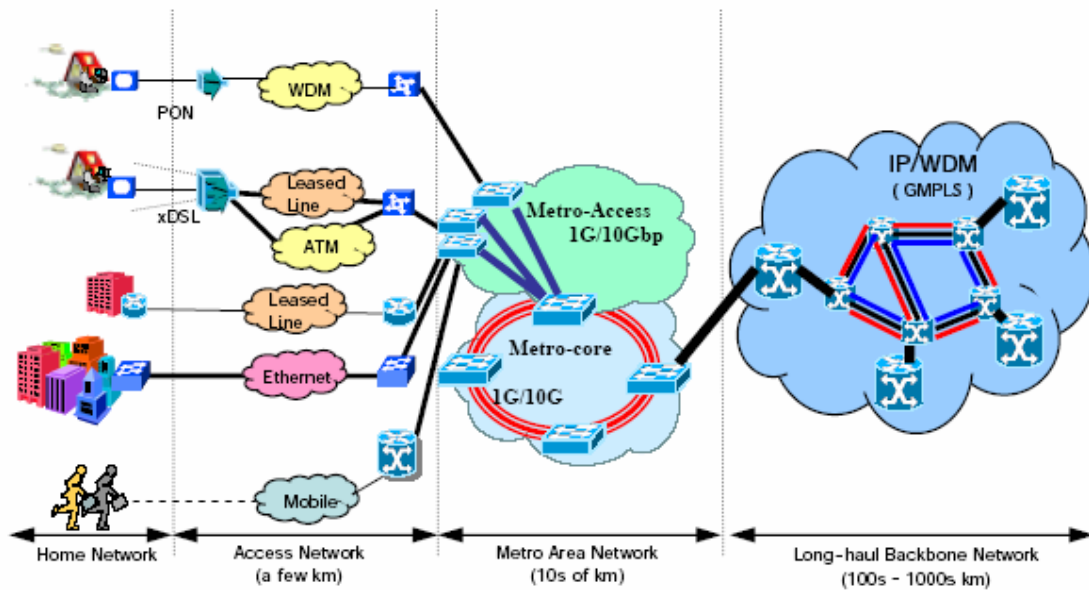


Figure 2.17: The end-to-end view of a possible future optical network: the access network, the metro network, and the long-haul backbone network [28].

## Chapter 3

# Optical network topologies

### 3.1 Introduction

This chapter will give a brief overview of the main types of optical network topologies in use today. The reasons why there is not a single standard network topology are numerous: countries have big differences in geographical features and the resultant distribution of major population centres, big differences exist in the amount and level of installed infrastructure, and the varying quality of service the telecommunications provider is contractually expected to provide.

Before the basic topologies are discussed, it is necessary to define the terminology that will be used in this chapter as well as in the rest of this dissertation. In mathematical graph theory, you have a graph that consists of a collection of vertices (singular – vertex). The connections between these vertices are called edges [29]. However, this terminology is not normally used by fiber optic network designers. Optical network engineers rather refer to networks, nodes, links, spans and paths. A node is defined as a point in the network where a signal is generated, switched or terminated. A link, also called a span, is defined as the fiber optic cable that connects two nodes, as well as associated optical amplifying components. A network is a collection of these nodes and links. Please refer to table 3.1 for a comparison between graph theory and fiber optic network engineering.

Table 3.1: Comparison of graph theory and optical network terminology.

<b>Graph theory</b>	<b>Optical network terminology</b>
Graph	Network
Vertex	Node
Edge	Span
Edge	Link

Thus, we can refer to an optical network as  $O = (N, L)$  where  $O$  is the optical network as a whole,  $N$  is the set of nodes and  $L$  is the set of links. A path is defined as the sequence of distinct links that connects two source-destination nodes in the network. Note that there may be more than one path per pair of nodes. Each link can also be assigned a weight that can be determined by a variety of characteristics, such as traffic carrying capacity, length of link or congestion. Each path can also be assigned a cost: this refers to the sum total of all weights along that path. This cost characteristic is crucial when it comes to determining which path between two points is the optimal path.

## 3.2 Network topologies

### 3.2.1 1 + 1 DP networks

In some networks, it is crucial that in the event of a fiber link or associated equipment failure, the traffic can be restored as quickly as possible (less than 30ms) [30]. These networks are generally given the name 1 + 1 DP (disjoint path) networks. A 1+1 DP network has a dedicated backup-connection for every connection in the network. In other words, for every connection between transmitter and receiver, an alternate or backup path is assigned that traverses a different physical route and utilises physically different fibers than the primary path.

In some configurations of this type of topology, the same signal is carried on both the primary and alternate paths, with the receiver concurrently monitoring both signal paths, and choosing the signal with the lowest bit error rate (BER). In another common configuration, the primary path is assigned as normal, but the alternate path might be assigned to carry lower priority (and thus lower money earning) traffic. This lower priority traffic is discarded the moment the receiver detects a failure on the primary path, with the rerouted primary signal taking its place.

The advantages of the 1 + 1 DP topology are speedy and assured restoration, but the disadvantages are inefficient use of network resources and high cost, since this topology requires an additional investment of 100% with regard to fiber redundancy [31].

### 3.2.2 The path-switched ring

It has historically been common for SDH or SONET configurations to be configured in a ring topology. A path-switched ring (PSR) topology has a number of nodes, with each of the nodes being connected to 2 other nodes, to form a ring-like structure. The data signal can travel clockwise around the ring, in which case the ring is called unidirectional. If the normal data signal travels both clockwise and anticlockwise, the ring is called bidirectional. Two architectures have become popular for SONET architectures:

- two-fiber, unidirectional, path-switched ring (two-fiber UPSR), and
- two-fiber or four-fiber, bidirectional, line-switched ring (two-fiber or four-fiber BLSR).

The SDH equivalent to BLSR is the multiplex-section shared-protection ring (MS-SPRing) [32].

In the event of a ring failure, PSRs typically provide restoration in between 50 and 150 milliseconds. PSRs are popular in legacy fiber applications, both long distance and metropolitan. PSRs generally provide better economics than 1+1 DP networks, due to the decrease in the total length of fiber optic cables needed to connect all nodes in a network of this topology.

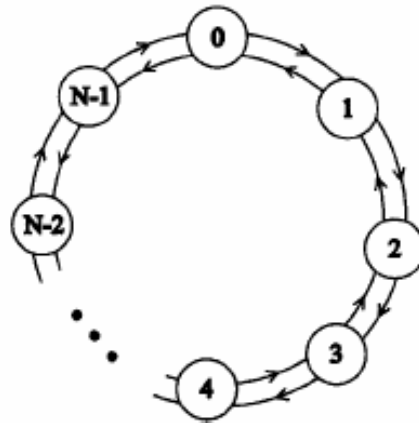


Figure 3.1: A two-fiber, unidirectional, path-switched ring (two-fiber UPSR) topology with one working and one protection path [33].

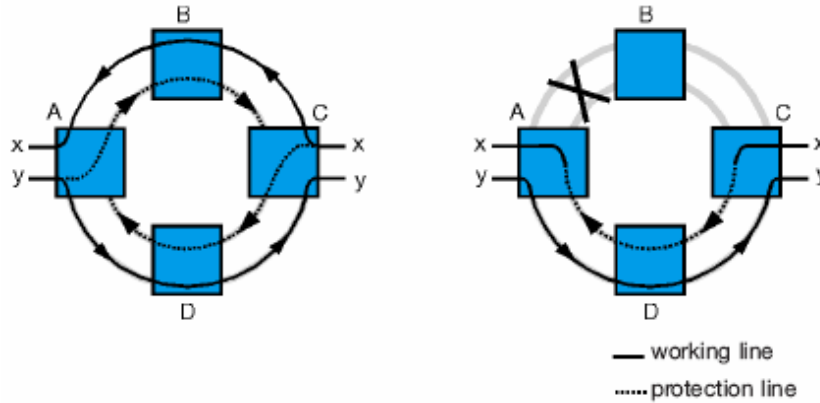


Figure 3.2: Illustration of protection in two-fiber UPSR topology [34].

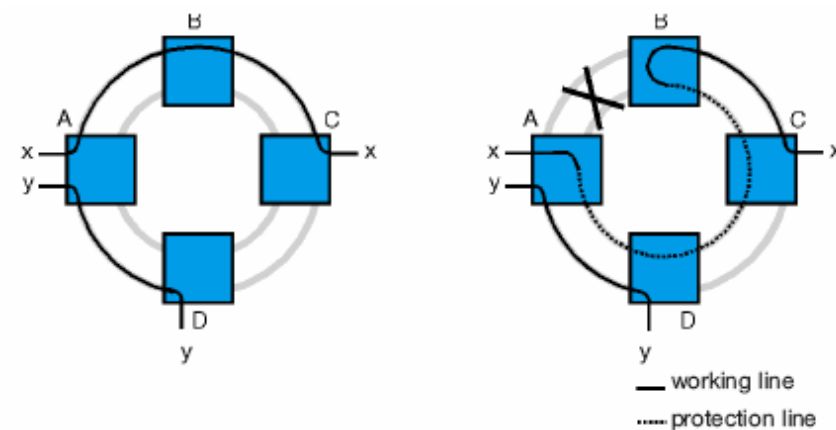


Figure 3.3: A two-fiber, bidirectional, line-switched ring (two-fiber BLSR). [34]

If one of the links is cut, traffic can be rerouted in the other direction. The advantages are speedy recovery and assured restoration, but the disadvantages are inefficient use of network resources. For some network topologies it is also not practical to connect all the nodes to a ring.

### 3.2.3 The mesh topology

The optical network topology that has been gaining more and more momentum in recent years is the mesh topology. This is primarily due to the mesh topology's more efficient use of network resources.

The mesh topology is characterised by the fact that each node is connected to two or more other nodes. In the extreme case where every network node is directly connected to every other network node, this topology is called a fully connected mesh topology. From a reliability and a traffic capacity point of view, this network would be ideal: in the event that a link is cut, traffic can easily be redirected onto a multitude of alternate paths. Because every link only carries the data that is intended for those two nodes, carried traffic per link is low and leaves lots of overhead for future traffic expansion.

A fully connected mesh topology consisting of  $N$  nodes, requires

$$\frac{N * (N - 1)}{2} \quad (3.1)$$

links. From a financial point of view this topology does however not make sense at all: capital expenditure and operational expenditure are huge. This stems from the enormous number of fiber optic cables that have to be installed in the beginning, and the related maintenance of it. The fully connected topology is thus rarely seen, except when a few nodes need to be connected that are geographically close to one another.

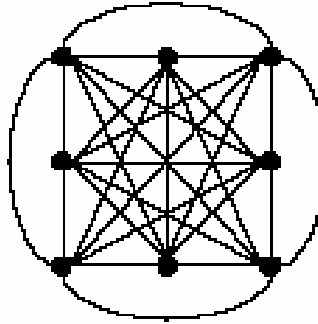


Figure 3.4: Example of a fully connected mesh topology [36].

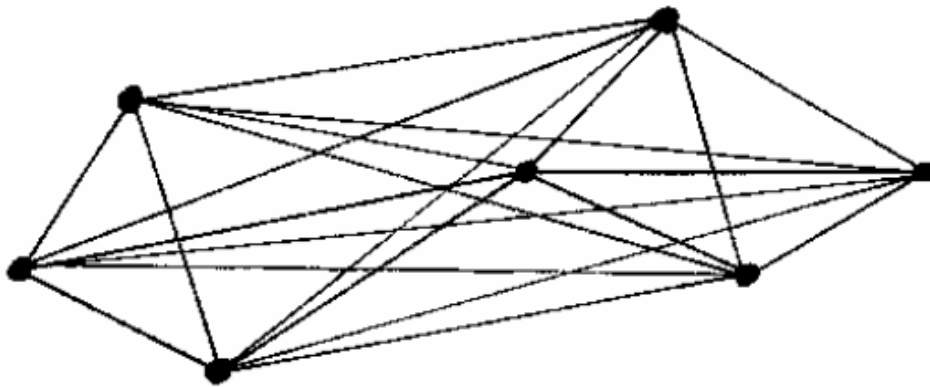


Figure 3.5: Example of a fully connected mesh topology [37].

In the other mesh topology extreme, every node is connected to only two other nodes, and this is called a sparsely-connected mesh topology. This variation is commonly found in the early stages of fiber networks, when all planned interconnect links have not yet been installed. In large geographic areas with few big towns, sparse networks are also commonly found. The ring topology can also be seen as a sparsely connected network, since each node is connected to two other nodes. The advantages are low initial and maintenance costs, but the restoration options are rather limited due to the limited number of links.

The connectivity factor of a network is defined as the average number of links per node, and can be calculated by the formula

$$d = 2*(L/N) \quad (3.2)$$

where  $d$  is the connectivity factor,  $L$  is the total number of links in the network and  $N$  is the total number of nodes in the network. The connectivity factor is also sometimes called the nodal degree of the network.

Figure 3.6 shows a conceptual example of a sparse network. While not qualifying as a fully sparse network (2 links per node) it comes close, with a connectivity factor of only 2.2 [38].

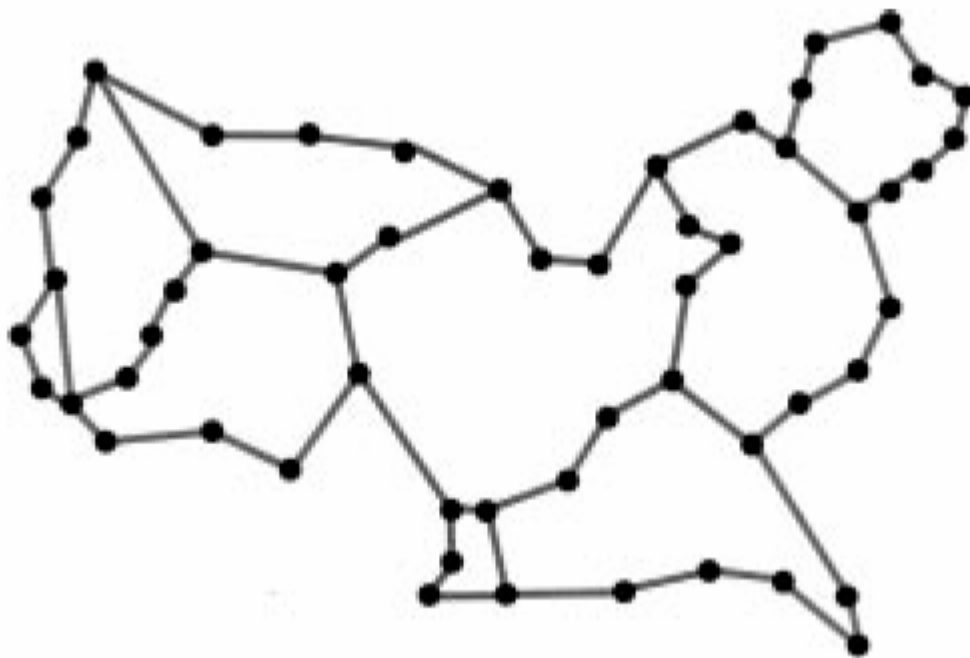


Figure 3.6: Conceptual example of a sparsely connected mesh topology [38].

It is interesting to note that European networks commonly have connectivity factors in excess of 4, while American and Canadian networks generally have connectivity factors approaching 3. This is due to the distribution of major population centres: European cities tend to be close to one another, while American and Canadian cities are spread out over very large geographical areas. This can be illustrated by the two following network topologies: figures 3.7 and 3.8. Figure 3.7 is the American NSFNET which consists of 14 nodes and 21 links (connectivity factor 3.0), and figure 3.8 is the European Optical Network, which consists of 11 nodes and 24 links (connectivity factor 4.54).



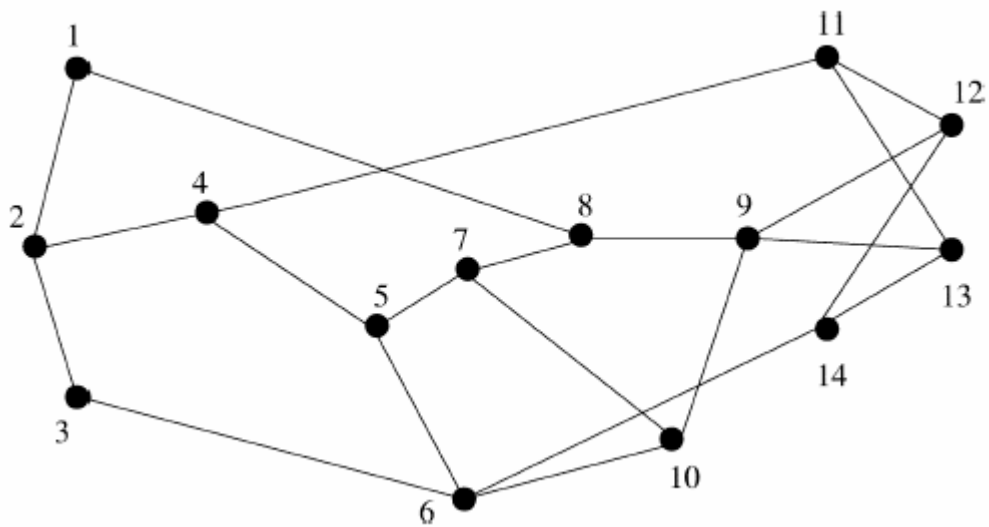


Figure 3.7: Topology of United States NSFNET: 14 nodes, 21 links, connectivity factor of 3.0 [4].

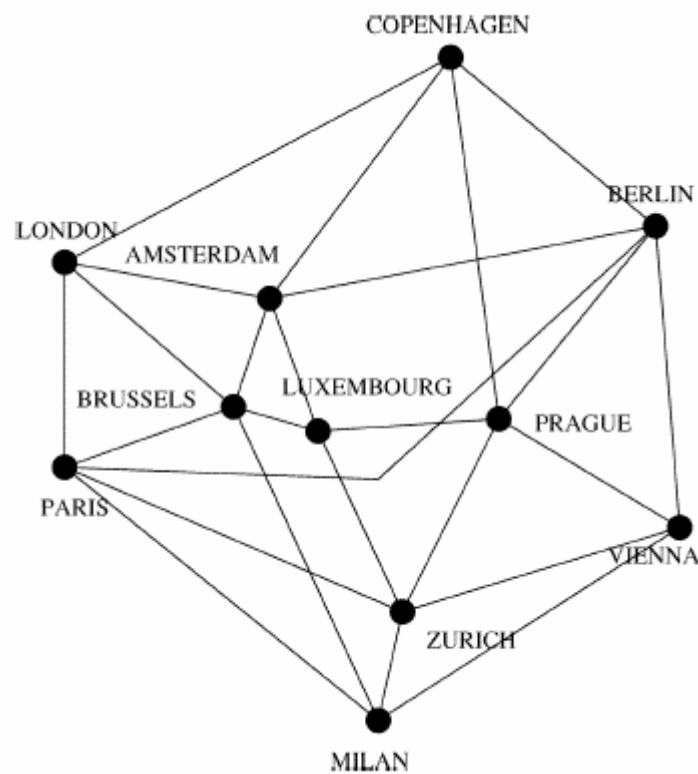


Figure 3.8: Topology of European Optical Network: 11 nodes, 24 links, connectivity factor of 4.54 [4].

Between the two extremes of sparsely connected meshes and fully connected meshes, there exists an opportunity for the network designer to design a network that has superior capacity efficiency to both 1+1 and PSRs, as well as costing less than 1+1 networks. Mesh networks achieve this by allocating link capacity intelligently, i.e. by assigning additional protection and restoration resources only when it is actively needed, thus freeing up bandwidth for revenue-generating traffic. By using the network resources more efficiently, costly network upgrades can also be postponed.

All these advantages come at the expense of increased network management complexity. The possibility also exists that traffic restoration time can increase considerably over 1+1 networks and PSRs (seconds compared to less than 50ms, if handled improperly).

To summarise: a mesh-based network has a number of nodes, with each of the nodes being connected to one or more of the other nodes. This topology has the distinction of allowing the traffic a variety of routes between the source and destination nodes. The advantages are efficient use of network resources and reduced cost, but the disadvantages are slower recovery times and increased complexity of network management and planning.

Figure 3.9 illustrates the DFN network (*Deutsches Forschungsnetz*, or the German Research Network) [39]. This is a good example of a typical modern mesh-based optical network. The highest speeds are found between the largest cities, with lower capacity links connecting the smaller cities. Some of the smaller towns are only connected to the network with one physically diverse link: if this link is damaged, it is impossible to reconnect the node to the network without the link being physically repaired. This is in stark contrast to a city like Berlin: this node is a major connecting hub that has 7 links connected to it.

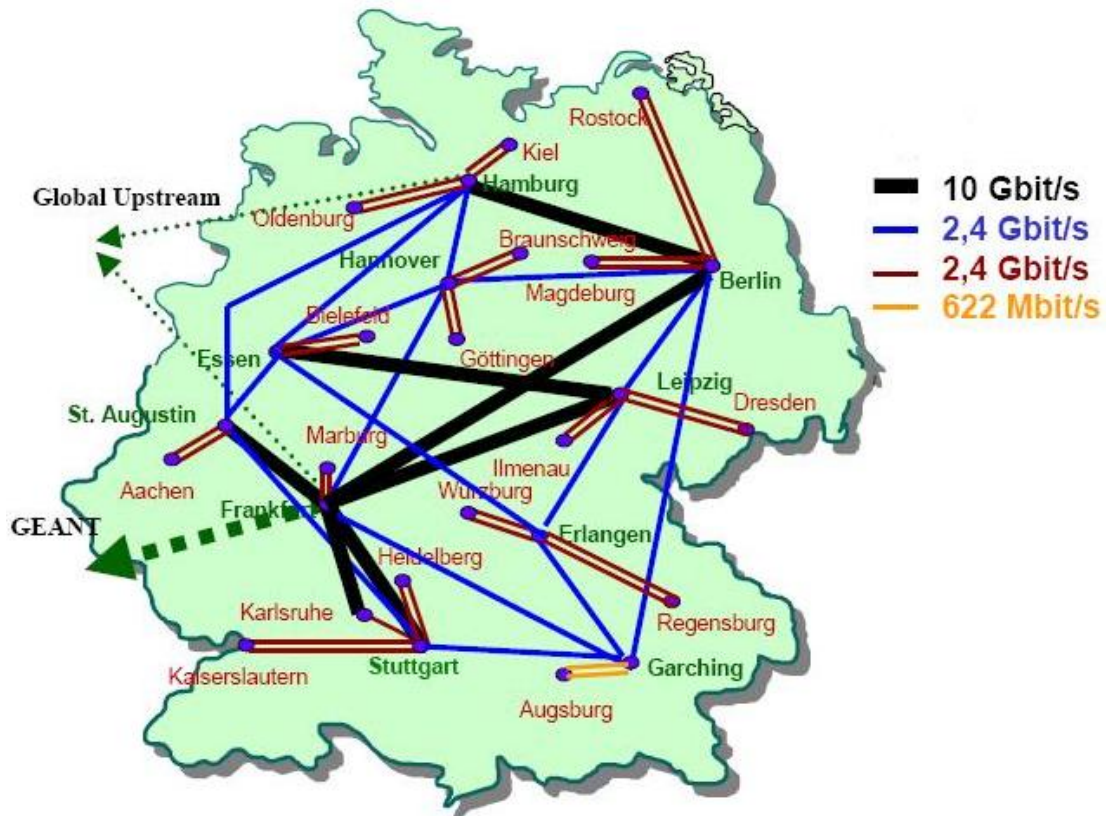


Figure 3.9: Topology of the DFN network (*Deutsches Forschungsnetz*) [40].

### 3.2.4 Special topologies

While most topologies can be classified as 1+1 DP, ring or mesh, there are always one or two exceptions. One of these is the undersea fiber optic cable. This usually takes the form of a linear topology, with extensions of the cable landing at certain coastal points. The reason for this topology is the prohibitive cost of buying and installing submarine fiber cable: it is considerably cheaper to repair the existing fiber than to install a backup cable.

Figure 3.10 shows the SAT-3/WASC/SAFE (South Atlantic Telecommunications cable no. 3 / West African Submarine Cable / South Africa Far East) cable that extends from Portugal to Malaysia, traversing Africa, for a total distance of 28 800km. It connects 15 countries, and makes a landing at 16 places. A backup cable of this length would be

prohibitively expensive. A ship is stationed midway around the route at Cape Town, and in the event of a fiber breakage the ship can normally repair the damage within a few days. This ship, named the Chamarel, is responsible for maintenance on the cable on the whole of the west coast of Africa and on the east coast up to Diego Garcia.

Recently, the SAFE cable was damaged by the tsunami of 26 December 2004. The cable broke approximately 300 km to the west of Banda Aceh in the Indian Ocean at a depth of 4000 m. Due to a shortage of specialised fiber optic repair ships at Singapore, repairs to the cable was only completed on 13 January 2005 [41].

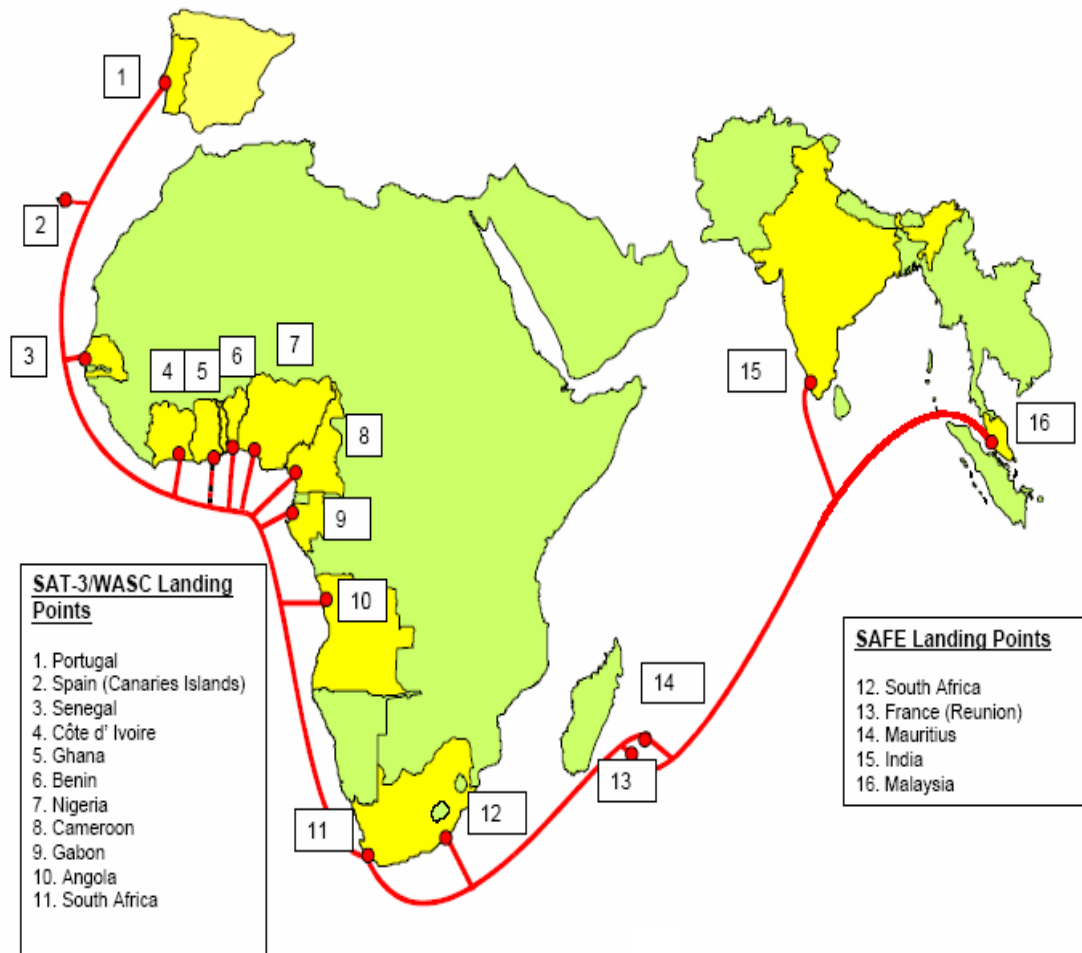


Figure 3.10: Topology of SAT-3/WASC/SAFE undersea fiber optic cable [42].

# Chapter 4

## Protection and restoration

### 4.1 Introduction

Restoring service after a failure has occurred is an important issue in optical network engineering. This is even more important if it is taken into account that the telecommunications service provider and the customer typically enters into an agreement in which the level of service is specified. The level of service for carrier-grade networks typically state that the customer is guaranteed a network uptime of 99.999% per year – the so-called five nines - which means that the customer may experience a maximum of 5 minutes of network downtime per year before penalties have to be paid out [43]. It is thus of utmost importance that a network must be *survivable* – in other words, be able to provide continued service in the presence of failures.

Any number of components may fail in an optical network – laser diodes may burn out, photodiodes may cease to receive, optical amplifiers may malfunction, power interruptions may occur and optical fiber cables regularly experience damage of some form. Considering that a fiber optic link can carry upwards of one Tbps of traffic that includes voice calls as well as data traffic, any interruption in service may adversely impact hundreds of thousands of people.

The network designer has to take various factors into consideration when deciding on a service backup plan during the designing phase of the network. These include, but are not limited to:

- Expected restoration time,

- Quality of service (QoS) to be supplied to the customer,
- Cost of installing and maintaining the necessary equipment,
- Whether the backup plan should be of a centralised or decentralised nature,
- And whether the backup plan would be able to scale well to keep up with expected future traffic volumes (“future proofing”).

## **4.2 SONET / SDH and the OSI protocol stack**

It can rightly be asked why there is a need for protection and restoration in optical SONET and SDH systems, since there are protocols in the 7-layer open systems interconnection (OSI) protocol stack that make provision for the rerouting for data in the event of a communications failure.

The OSI reference model was developed by the International Organization for Standardization (ISO) to provide a framework for the development of protocol standards. The intent of the OSI model is to allow one or more protocols to be developed for every layer, and that these protocols could function independently from the layers below or beneath it. Table 4.1 lists the seven layers along with a brief description of every layer.

Table 4.1: The 7-layer OSI protocol stack [44].

Layer number	Layer name	Description
7	Application	Provides access to the OSI environment for users and also provides distributed information services.
6	Presentation	Provides independence to the application processes from differences in data syntax.
5	Session	Provides the control structure for communication between applications. Establishes, manages and terminates connections (sessions) between co-operating applications.
4	Transport	Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.
3	Network	Provides upper layers with independence from the data transmissions and switching technologies used to connect systems; responsible for establishing, maintaining and terminating connections.
2	Data	Provides for the reliable transfer of information across the physical link; sends frames with the necessary synchronization, error control and flow control.
1	Physical	Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional and procedural characteristics to access the physical medium.

In the event of an optical communications fiber link failure, this corresponds to a failure in layer 1 (the physical layer) of the OSI model. SONET and SDH are level 1, although it also does error checking, which normally is a layer 2 (data link layer) task [45]. Protocols that support rerouting like IP is typically on level 3 (network layer). It is logical that the closer the protection and restoration mechanism is to the physical layer, the quicker the connection can be restored. This is partly due to the increase in overheads as you go higher up the OSI stack. This means that using layer 1 SONET/SDH for protection instead of level 3 ATM or IP is the difference between hundreds of milliseconds versus seconds (ATM) to several minutes (IP).

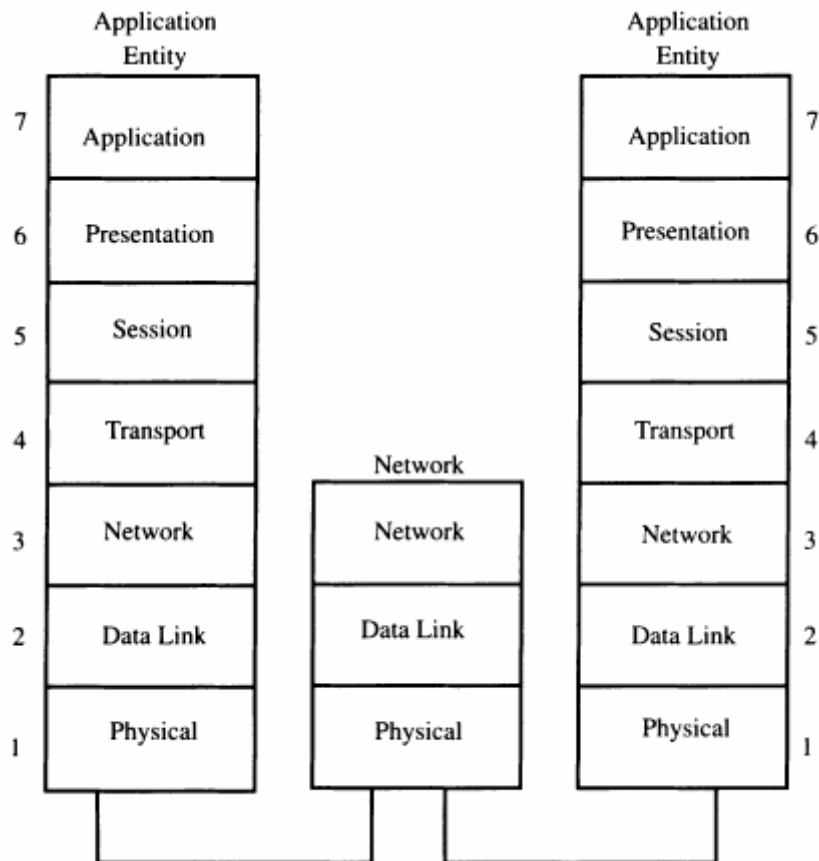


Figure 4.1: Two network entities (end nodes) are typically connected by switching devices that only implements the first three layers of the OSI protocol stack [46].



When it comes to network design with regards to the OSI model, you will normally only find the first three layers (physical, data and network) present in the hardware that resides in the nodes. The other four layers (transport, session, presentation and application) are normally provided by the computers and their associated software of the end users at the source and destination nodes.

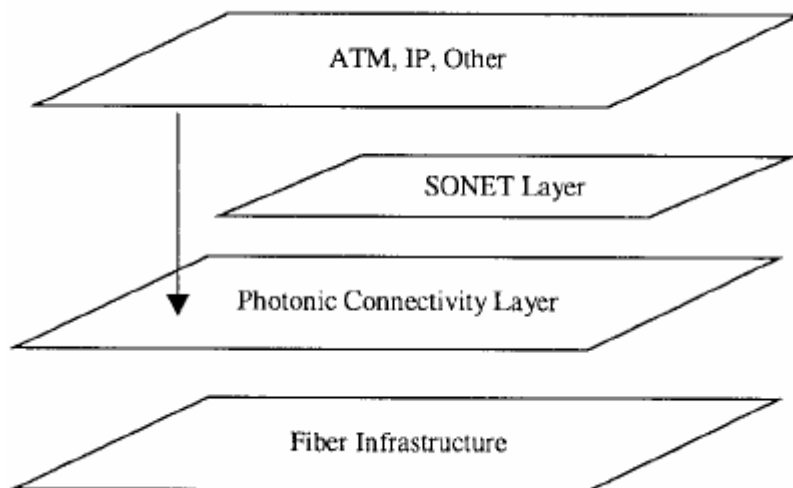


Figure 4.2: Example of a typical optical network protocol stack [47].

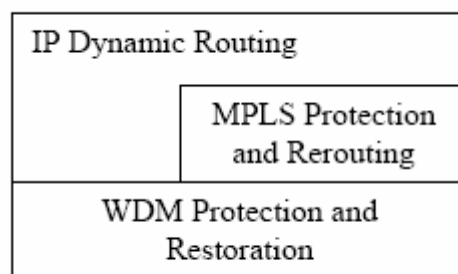


Figure 4.3: Survivability at IP/MPLS/WDM layers [28].

### 4.3 Routing and wavelength assignment

Routing and wavelength assignment (RWA) is a vitally important part of the network designer's arsenal. The RWA method or algorithm the designer chooses can influence network performance factors such as protection or restoration time and capacity efficiency.

Routing and wavelength assignment, as the name implies, relates to the routing of, and the assigning of, the multiple different wavelengths that make up the typical WDM system. The available wavelengths in a system have to transport the data from multiple source-destination pairs in the most efficient way possible. The RWA algorithm has to take factors into account such as:

- The maximum number of wavelengths available per link (and this may differ considerably from link to link).
- Is wavelength converting capability available at the node?
- The shortest route with the least number of hops will introduce the lowest propagation delay into the signal. The shortest route, however, may be congested and a longer route may have to be accepted.
- The shortest route will also utilise the least resources. If the network is extremely congested and a connection only has a very long route available, might it not be better to deny the request, and use those resources to establish multiple shorter connections?

### 4.3.1 Routing

One of the most popular algorithms for finding the shortest route between two paths in a network is called Dijkstra's algorithm (named after its discoverer, the Dutch computer scientist Edsger W. Dijkstra). The pseudo code for Dijkstra's algorithm is shown below in figure 4.4.

```

for each vertex v in V[G]                                     //Initialization
    do d[v] = infinity
        previous[v] = undefined
d[s] = 0

```

```

S = empty set
Q = set of all vertices
while Q is not an empty set
    do u = Extract-Min(Q)
        S = S union {u}
        for each edge (u, v) outgoing from u
            do if  $d[v] > d[u] + w(u, v)$  // Relax (u, v)
                then  $d[v] = d[u] + w(u, v)$ 
                    previous[v] = u

```

Figure 4.4: Dijkstra's algorithm in pseudo code [48].

In Dijkstra's algorithm, it starts at one node (the first level), and determines which nodes are connected to the first node. From this second level of nodes, it then looks to the nodes that are connected to the third level. At each step of the process, the weight (cost) of the path up to that point is updated. This is also called the relaxation process. This process continues until the list of destination nodes has been exhausted, in other words the shortest paths have been found from the source node to all of the other nodes in the network. The algorithm can be likened to the form of a spanning tree.

It is thus interesting to note that determining the shortest route from the source node to the destination node actually also produces the shortest routes from the source node to all the other nodes in the network as well.

The default cost per link is normally taken as 1. If a link is congested, its cost might be adjusted to a value of more than 1. This will encourage Dijkstra's algorithm to select a path that might be a bit longer, but less congested.

Dijkstra's algorithm is also commonly used in Internet routing. In both Internet and optical network routing, the implementation is commonly known as open shortest path first routing (OSPF).

There also exist many other routing algorithms. Some of these include:

- The Bellman-Ford algorithm (can be used on networks with negative link weights) [49].
- Least-loaded routing (LLR) [50, 51].
- Minimum interference restorable routing (MIRR) [52] etc.

These algorithms will give different results depending on network topology and traffic levels.

### 4.3.2 Wavelength assignment

After the (normally) shortest route between the various source-destination pairs have been established, the RWA algorithm has to determine which wavelengths to allocate to which links and routes.

The most widely used wavelength assignment algorithm is the “first-fit algorithm”. The first-fit algorithm gives all wavelengths on a link an arbitrary number from 1 to N, where N is the maximum number of wavelengths on that particular link. Note: the same arbitrary numbering scheme must be used on all links in the network, otherwise the algorithm decreases in efficiency. It is normal to number wavelengths according to wavelength: 1530.04nm would be number 1, 1530.24nm would be number 2 etc.

When a wavelength needs to be allocated, the wavelength with the lowest arbitrary number, in this case 1, is allocated. The second request will be allocated wavelength number 2 etc. Thus the wavelength with the lowest number will always be allocated first. The idea behind this algorithm is to try to keep the wavelengths on a path, from the source to the destination, the same across multiple links. This is especially important in networks with nodes without wavelength conversion capability.

Another wavelength assignment algorithm is the “random wavelength selection algorithm”. Once again, all wavelengths are allocated arbitrary numbers from 1 to N, and

wavelengths are allocated at a random basis. However, since the random wavelength selection algorithm generally delivers higher blocking probabilities than the first-fit algorithm, it is generally not used in non-wavelength-converter equipped networks. In wavelength-converter equipped networks, the performance is similar.

The “most-used algorithm” allocates wavelengths according to their utilisation: the most-utilised wavelengths get allocated more in future. This ability to use historical data allows the most-used algorithm to perform slightly better than the first-fit algorithm in ring topologies: however, in mesh-based topologies, the performance is similar [50].

## **4.4 Protection and restoration**

### **4.4.1 Protection in 1+1 DP and path-switched ring (PSR) networks**

Protection in 1+1 DP and path-switched ring networks are generally straightforward. In 1+1 DP networks, the same data signal is sent over two physically separate paths to the destination. At the destination, the receiver monitors both data streams concurrently and chooses the one with the lowest bit error rate. In the case of failure of one of the signals, the receiver automatically switches over to the alternate signal.

Path-switched rings send the signal around the ring (generally clockwise during normal operation). In case of a failure in one of the links, the signal is automatically switched to go the other way around the ring (generally anti-clockwise).

In both of the above scenarios, the signal switching (normally via OXC) takes place almost instantaneously. Since there are only two choices in a 1+1 DP network (path 1 or path 2) and two choices in a PSR (clockwise or anti-clockwise), no real intelligence is required to make this protection scheme work. Both protection schemes are called automatic protection switching (APS). Examples of a generalised APS scenario and APS in a 4-fiber BLSR are shown in figures 4.5 and 4.6 on pages 47 and 48 respectively.

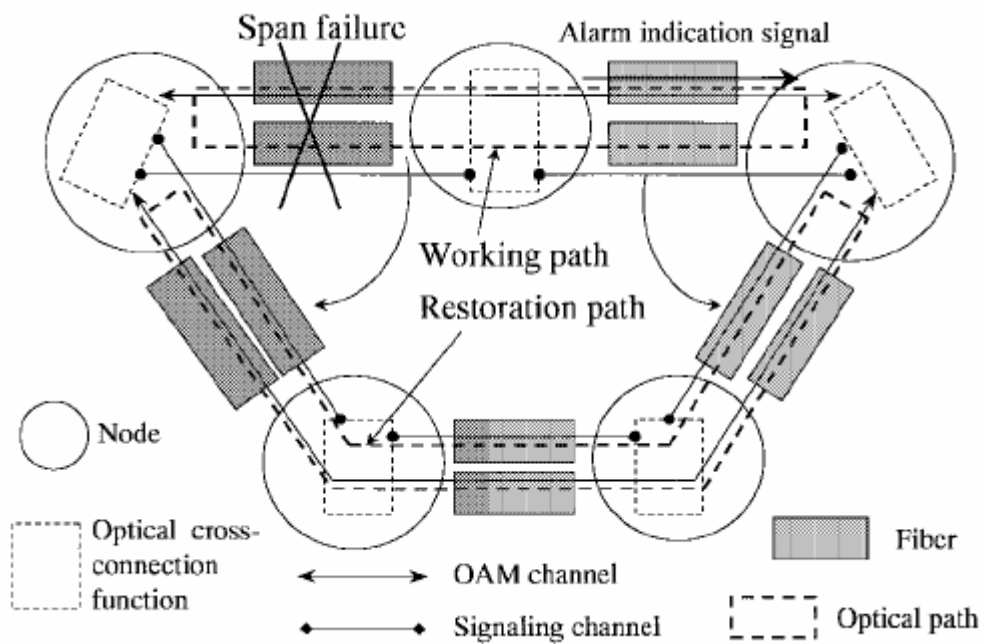


Figure 4.5: APS in a path-switched ring topology that makes use of an operations, administration and maintenance (OAM) channel [53].

Since this dissertation will focus on restoration and protection in mesh-based network topologies, APS falls outside the scope of this dissertation and is thus mentioned for informative purposes only.

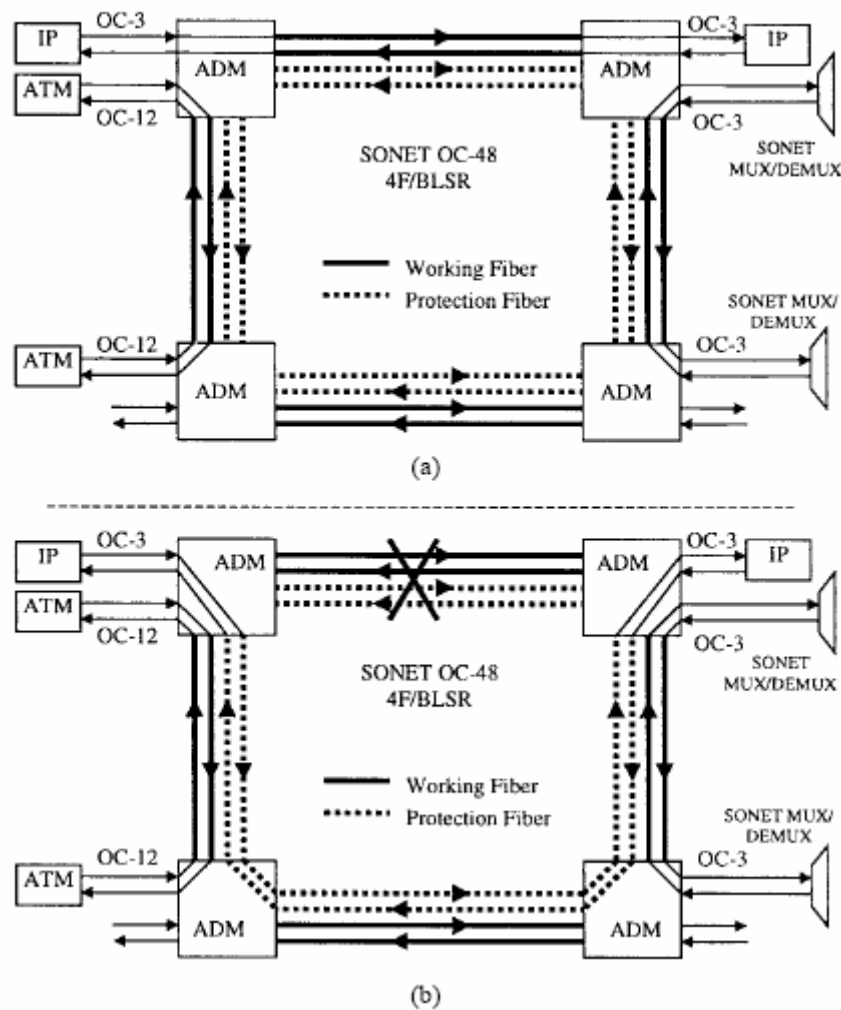


Figure 4.6: Operation of APS in a four-fiber BLSR. Operation in (a) is normal operations, while (b) is after a failure has occurred [47].

#### 4.4.2 Protection and restoration in mesh-based optical network topologies

Protection and restoration in mesh-based optical network topologies can take on a multitude of forms, due to the large number of alternate paths available in mesh-based networks. Depending on whether the network designer is designing the network for performance, low cost, or any point in between, a multitude of options are therefore available.

In some texts, the terms protection and restoration are used interchangeably. To clear up any ambiguities that might arise, the next two paragraphs will define protection and restoration as used in this dissertation.

In this work, *protection* will be defined as spare network capacity that is put aside whenever a connection is made between two nodes in a network. In other words, along with the RWA for the primary path, a RWA for the alternate path is also determined. This spare network capacity can either be dedicated, in which case the set-aside resources remain free of traffic, or the resources can be shared, in which case other, normally lower priority, traffic is allowed on the set-aside resources, but removed from it when needed.

In this work, *restoration* will be defined as an act which tries to make an alternate route available to a connection only after a link failure has occurred. Spare capacity is *not* put aside at connection setup, but only allocated when needed. In other words, when a source-destination pair is set up, only the primary route and wavelength assignments are configured. If the network detects a link fault, only then is an alternate route and wavelength assignment computed. As can be expected, this computation has to take into account the traffic throughout the network, and an alternate route might not always be available in a heavily congested network. If this is the case, the connection will be broken.

Figure 4.7a and 4.7b illustrate the difference between path protection and link protection. In figure 4.7a, path protection is utilised. At the setup of the connection between nodes 1 and 6, the following route is designated as the primary route: 1-2-3-6, and route 1-4-5-6 is designated as the backup route. It is important to note that these two routes are path-disjoint: that is, the primary and the backup routes do not share any individual links. If a failure of the primary route is detected, the data signal is switched to the backup route.

In figure 4.7b, link protection is utilised. At the setup of the connection between nodes 1 and 6, the following route is designated as the primary route: 1-2-3-6. The routing algorithm also determines how to route the signal around every possible link failure site in the event of a link failure. In the event of the link between nodes 2 and 3 experiencing a



failure, the traffic is only rerouted around the broken link. In this scenario, the backup route will be 1-2-4-5-3-6. It is important to note that the primary and backup paths in the link protection mechanism are not path-disjoint.

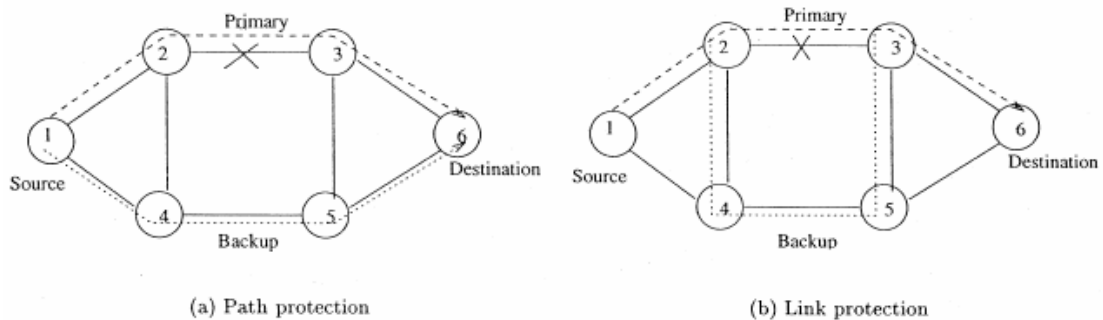


Figure 4.7: Differences between path protection (a) and link protection (b) [54].

Path protection is generally more capacity efficient than link protection due to the fact that it distributes replacement paths over a wider area of the available network. However, as path protection has to find routes between numerous source-destination pairs as opposed to link protection where traffic only has to be rerouted around the broken link, path protection is more complex [55].

Restoration is more complex than protection. Due to the varying levels of network traffic as well as varying numbers of connections, the network might be extremely congested, very quiet or at any stage in between when a network fault occurs. The restoration algorithm must be able to successfully reroute traffic, even in a congested network with few spare resources.

A possible routing and wavelength assignment algorithm is called the “flow formulation algorithm”. The flow formulation algorithm calculates all possible paths between a source-destination pair, as well as taking into account the traffic on all links in the network. A related algorithm is called the “path formulation algorithm”. This algorithm only considers a small number  $k$  of shortest paths between a source-destination pair, as well as taking into account the traffic on all links in the network. The path formulation algorithm delivers results that are nearly as good as the flow formulation, while requiring  $N$  times less

computations, where  $N$  is the number of nodes in the mesh. This is due to the fact that shorter paths are generally more capacity efficient than longer paths, requiring less resources [50].

To determine optimal routing and wavelength assignments in the face of ever-changing network conditions is no easy task. One way to determine optimal restoration RWAs is the “multi commodity maximum flow” (MCMF) problem [32]. MCMF takes into account possible paths as well as traffic volumes. MCMF, however, makes use of linear programming (LP), which gives fractional answers [32]. WDM, by its nature, is not a fractional system. In other words, you can only have an integer number of wavelengths on any link (1, 2, 3, etc. but not 1.1, 4.45 etc). The answers derived from MCMF will thus be close to the optimal answer, not the perfect one.

Due to the large computational complexity in solving LP problems, it does not scale well to networks with large numbers of wavelengths, links and nodes [50]. To solve the optimal MCMF in a network containing 53 nodes and 79 links with a connectivity factor of 2.98, took 1.2 days on a DEC Alpha workstation [55]. Even though this was a worst case scenario using maximal accuracy, and taking Moore’s law into account (computational power doubles roughly every 18 months), the MCMF and associated LP is unlikely to become a big factor in restoration, which requires rerouting in under 2 seconds. In fairly static networks requiring protection rather than restoration, MCMF might be a viable option and is used when maximal capacity efficiency is required.

A taxonomy of survivability, showing all flavours of protection and restoration, is shown on the next page as figure 4.8.

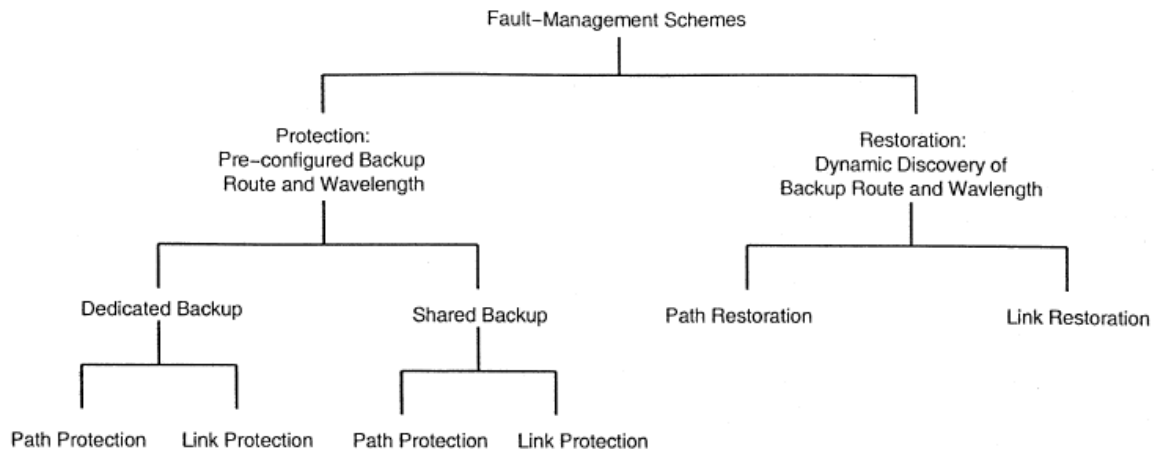


Figure 4.8: Taxonomy of survivability with regard to protection and restoration [54].

#### 4.5 Centralised vs de-centralised (distributed)

There are two options in deciding on the runtime configuration of the RWA algorithm, namely centralised or distributed.

With the centralised approach, every network has a control center, which houses the computers and databases that controls the whole network. The computers are needed to provide computational power for the RWA algorithm, while routing tables are maintained in the databases. With this approach, the nodes themselves have only limited intelligence, and their associated internal OXCs will only change their configuration when instructed to do so by the control center.

The control center does not have to be directly connected to every single node in the network, instead, it relies on monitoring traffic between all the nodes: SONET and SDH can put link monitoring information in available overhead bytes. This information travels from node to node, reaching the control center after a few hops. This link monitoring information typically only contain the status of the links, and takes up very little bandwidth. Due to the fact that a damaged link will carry no information at all (if the monitoring information and data share the same physical fiber), low bandwidth radio

frequency (RF) links are sometimes used to convey monitoring data to the control center. Link status information can also be obtained by analysing the BER of the received signal, by monitoring the received strength of the pumping laser in EDFA systems, or by measuring the received strength of the optical supervisory channel.

In some optical systems, an optical supervisory channel (OSC) is sometimes assigned to the system. The OSC is responsible for the operation, administration, maintenance and provisioning (OAM&P) of the network. The OSC consists of an additional wavelength outside the normal WDM range that exists in an optical fiber that carries no data. Instead, it carries control and management information. The OSC, when utilised, thus serves as the primary signaling channel between network elements [47].

With the de-centralised (also called distributed) approach, the RWA algorithm is taken out of the control center and put into every node in the network. Every node contains enough processing power to power the RWA algorithm, and routing tables are kept. These routing tables can either be basic, with just the information on the nearest nodes, or comprehensive, in which case the routing tables contain a multitude of information regarding primary as well as alternate routes in the network. The number of entries in a typical modern backbone network node's routing database may contain between 50000 and 100000 entries [56]. It must be noted that although the OXCs in the nodes may be controlled locally, network monitoring information is still given through to a central control center. This is due to the fact that the network operation personnel still need to have an overview of what is going on in the network. If need be, they can instigate different routing paths, in effect overruling the local nodes. This can be important in repair, and resultant testing scenarios.

With a distributed algorithm, if two connected nodes detect a failure between them, the restoration algorithm is initiated. The two nodes are designated "Sender" or "Chooser" at random [38]. The Sender node starts sending out packets of information (sometimes called "statelets") on the remaining functional links, with the packets containing the following information:

- Source node,

- Destination node,
- History of the route traveled up to that point,
- Timer value,
- And hop count.

At the arrival of the packets at each new node, the destination field in the packet becomes the source field, the hop count gets incremented, the timer gets incremented and the history of the route traveled up to that point gets amended. The node then sends out a copy of this packet (with a different destination field) to all of the connected links on that node, with the exception of the link it received the packet from. This spanning tree process continues until the Chooser node is reached [57]. It is important to note that the Chooser node receives multiple packets and thus multiple possible routes, and has to choose which route to accept. Normally this is the shortest route.

After choosing a particular route, the Chooser node then sends back a packet along the reverse route, configuring each node and its associated OXCs along its path. This packet then reaches the original Sender node, thus establishing a new connection. This process is graphically illustrated in figure 4.9 on the following page. The timer value is used to prevent uncontrolled network congestion: after a certain timer value is reached, all Sender packets are discarded.

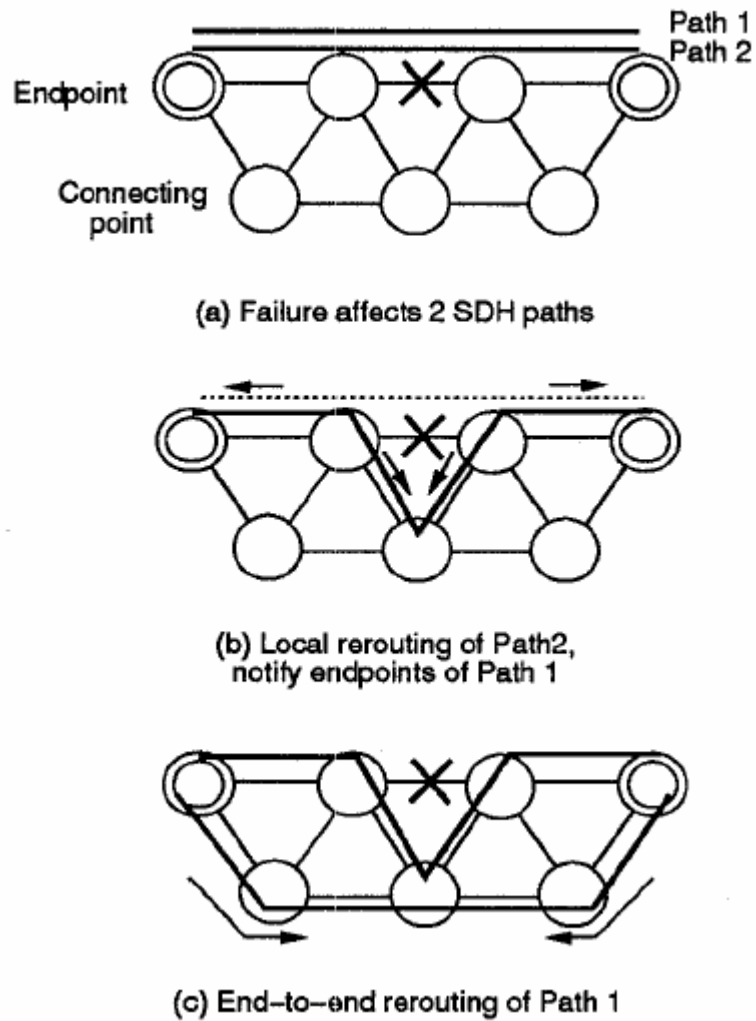


Figure 4.9: Process of restoration using the sender-chooser method [58].

## Chapter 5

# Network simulator packages

The use of simulation programmes capable of simulating complex optical networks has become crucial to the optical network designer. The ability to simulate different topologies, routing and wavelength assignments, and survivability aspects of optical networks ensures superior performance of the completed network.

### 5.1 Available network simulation packages

There are several available simulation packages that are capable of simulating large scale networks. Some of these include:

- NEST (available from Columbia University),
- REAL (available from Cornell University),
- BONEs (commercial release from Cadence Design System).
- OPNET (commercial release from MIL 3),
- NS (available from the University of California Berkeley),
- NS2 (available from the University of California Berkeley),

NEST stands for NEtwork Simulation Testbed, and is a network simulation tool that allows for the testing and simulation of distributed algorithms on distributed systems. It is written in the C programming language, and runs on the Unix operating system. The newest version of NEST is version 2.6, and the full source code is available from Columbia University [60].

However, as the package was last updated in 1988, it has been superseded by newer, more advanced packages and is thus considered obsolete.

REAL is a network simulator that allows the user to model and study the dynamic behaviour of flow and congestion control schemes in packet-switched data networks. Some examples of its functionality include transmission control protocol (TCP), fair queuing and hierarchical round robin scheduling. It has a modular system design, is written in the C programming language and is based on the NEST version 2.5 network simulator. The simulation package runs on most derivatives of the Unix operating system. The newest version is REAL5.0, and the full source code is available from Cornell University [61]. However, as the package was last updated in 1997, it has been superseded by newer, more advanced packages. Due to the lack of support and a dwindling user base, it is therefore not a good option.

BONeS (Block Oriented Network Simulator) is a commercial release from Cadence Design System. This network simulator allows for the simulation and analysis of a broad range of scenarios, including communication networks and distributed processing systems. The simulator has a graphical user interface (GUI), and is written in the C/C++ programming language [62]. The latest release is release 4.01.

The package was last updated in 1998. As this is a commercial release, modifying the source code may be problematic due to copyright issues. Therefore, this package is not a viable choice.

OPNET is a commercial release from OPNET Technologies, Inc. OPNET is a network simulator that is widely used by researchers, as well as by those in industry. Of particular interest is the following:

- It is available for free to universities,
- It contains a toolbox, WDM Guru, that is specifically adapted for use in fiber optic networks.



With the help of the WDM Guru toolbox, it is possible to investigate factors such as optimal optical regenerator placement on long-distance links, to predict future traffic growth and identify associated potential bottlenecks, and to look at the projected failure rates of various components in the network. OPNET has a graphical user interface and is fairly easy to use. A screenshot of the program is shown below in figure 5.1. The program is available from OPNET Technologies [63].

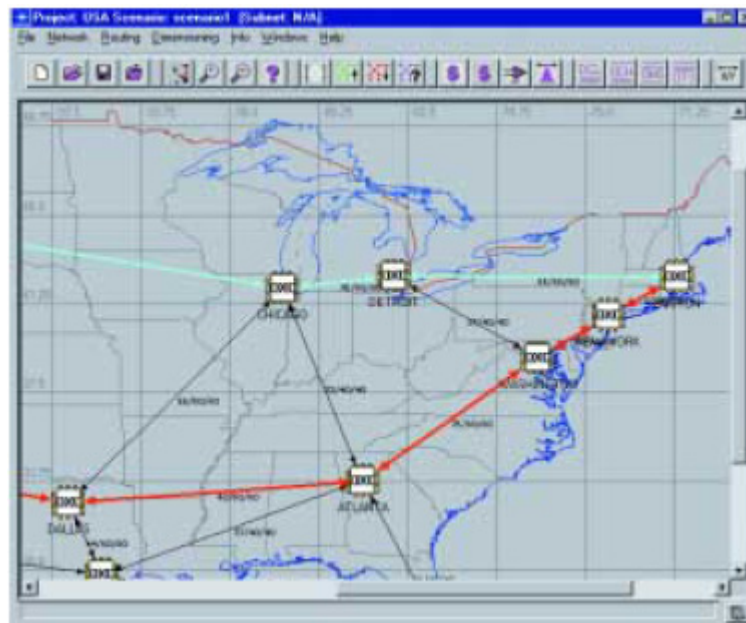


Figure 5.1: Screenshot of OPNET WDM Guru network simulator package [64].

The main drawback with this package is the fact that even though it is free for academic use, it is still a copyrighted product, and this may prove to be cumbersome and problematic when attempting to modify the source code.

NS (network simulator) is a network simulation software program, originally developed by a collaborative effort from the University of California Berkeley, Lawrence Berkeley National Laboratory and Xerox's Palo Alto Research Centre [49]. NS builds on the REAL network simulator and it is widely used by researchers worldwide. The program is Linux-based and is completely open source, and this has allowed many different individuals and organizations to contribute functionality to the program. The latest version of NS is version 1.0 of 1996, and it is available from the University of California Berkeley [65].

NS2 is the new and improved version of NS. Architectural changes have been implemented, amongst them three major ones:

- The more complex objects in ns have been decomposed into simpler components for greater flexibility,
- The configuration interface now consists of Otcl, an object-oriented version of Tcl,
- The interface code for the Otcl interpreter is separate from the main simulator [49].

After the addition of numerous modules and functionality, NS2 now supports numerous networking protocols, and is used to simulate satellite communications, cellular communications, local area networks, internet traffic etc. NS2 also makes up part of the virtual internet test bench (VINT) [66]. The most compelling fact of NS2 is the fact that the source code is in the public domain: that means anybody can take the source code and adapt it for his or her individual needs. People and organisations are contributing functionality towards NS2 on an ongoing basis: therefore new revisions are constantly released. The most recent version of NS2 is release 2.28 of 2005, and it is available from the University of California Berkeley [67].

## 5.2 NS2

After a thorough investigation of all the available simulation packages, it was decided to use NS2. The main reasons for this decision have to do with the open nature of the source code, as well as the broad worldwide user base.

NS2 is written in 2 programming languages, namely object tool command language (OTcl) and C++. OTcl is generally used to write the simulation script, while C++ is generally used to define, write and use the different algorithms and commands that will process large sets of data.

OTcl is an interpreted language, which means that the simulation code is interpreted one line at a time, every time the simulation is run. Although the interpreted nature of OTcl makes it run a lot slower than C++, it is not that important in less processing-intensive uses such as simulation configuration files. Here, the ability to let the researcher make numerous quick changes to the simulation configuration, without a lengthy compile process, is of more importance.

C++ is a compiled language, which means that the source code is translated into machine language only once, called the compilation process. This compiled machine language code is then executed every time the program is run. The compiled nature of C++ code makes it a lot quicker than the interpreted nature of OTcl code, and C++ is thus the preferred method of implementing processing-intensive tasks such as routing algorithms, statistical analyses etc.

NS2 can thus be viewed as a simulation package that makes use of a split-level programming approach [49]. The compiled language (C++ in this case) makes up the building blocks of the simulation (nodes, traffic models, protocols etc.) and the interpreted language (OTcl in this case) makes up the glue that binds the building blocks together. As with any other programming language OTcl is able to declare variables, execute loops, make branch decisions etc. The syntax is different to that of languages such as C or C++. Although it is possible to implement computationally intensive functions in OTcl, it is generally not recommended due to the slow execution time of its interpreted nature.

In the simulation configuration file, also called the simulation script, the researcher configures the simulation via OTcl. Elements such as nodes, links, protocols, timer values etc. are initialised, as well as relevant input and output files. Simulation scripts are normally entered via the keyboard, but interfaces have been developed that make use of a graphical, drag and drop interface [68]. An example of an NS2 script file that creates a 4-node network topology with associated traffic sources and sinks is shown in figure 5.2.

```
#Create a simulator object  
set ns [new Simulator]
```

```

#Define different colors for data flows
$ns color 1 Blue
$ns color 2 Red

#Open the nam trace file
set nf [open out.nam w]
$ns namtrace-all $nf

#Define a 'finish' procedure
proc finish {} {
    global ns nf
    $ns flush-trace
    #Close the trace file
    close $nf
    #Execute nam on the trace file
    exec nam out.nam &
    exit 0
}

#Create four nodes
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]

#Create links between the nodes
$ns duplex-link $n0 $n2 1Mb 10ms DropTail
$ns duplex-link $n1 $n2 1Mb 10ms DropTail
$ns duplex-link $n3 $n2 1Mb 10ms SFQ

$ns duplex-link-op $n0 $n2 orient right-down
$ns duplex-link-op $n1 $n2 orient right-up
$ns duplex-link-op $n2 $n3 orient right

#Monitor the queue for the link between node 2 and node 3
$ns duplex-link-op $n2 $n3 queuePos 0.5

#Create a UDP agent and attach it to node n0
set udp0 [new Agent/UDP]
$udp0 set class_ 1
$ns attach-agent $n0 $udp0

# Create a CBR traffic source and attach it to udp0
set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 500
$cbr0 set interval_ 0.005
$cbr0 attach-agent $udp0

#Create a UDP agent and attach it to node n1
set udp1 [new Agent/UDP]
$udp1 set class_ 2
$ns attach-agent $n1 $udp1

# Create a CBR traffic source and attach it to udp1
set cbr1 [new Application/Traffic/CBR]
$cbr1 set packetSize_ 500
$cbr1 set interval_ 0.005
$cbr1 attach-agent $udp1

```

```

#Create a Null agent (a traffic sink) and attach it to node n3
set null0 [new Agent/Null]
$ns attach-agent $n3 $null0

#Connect the traffic sources with the traffic sink
$ns connect $udp0 $null0
$ns connect $udp1 $null0

#Schedule events for the CBR agents
$ns at 0.5 "$cbr0 start"
$ns at 1.0 "$cbr1 start"
$ns at 4.0 "$cbr1 stop"
$ns at 4.5 "$cbr0 stop"
#Call the finish procedure after 5 seconds of simulation time
$ns at 5.0 "finish"

#Run the simulation
$ns run

```

Figure 5.2: Example of NS2 OTcl script file [69].

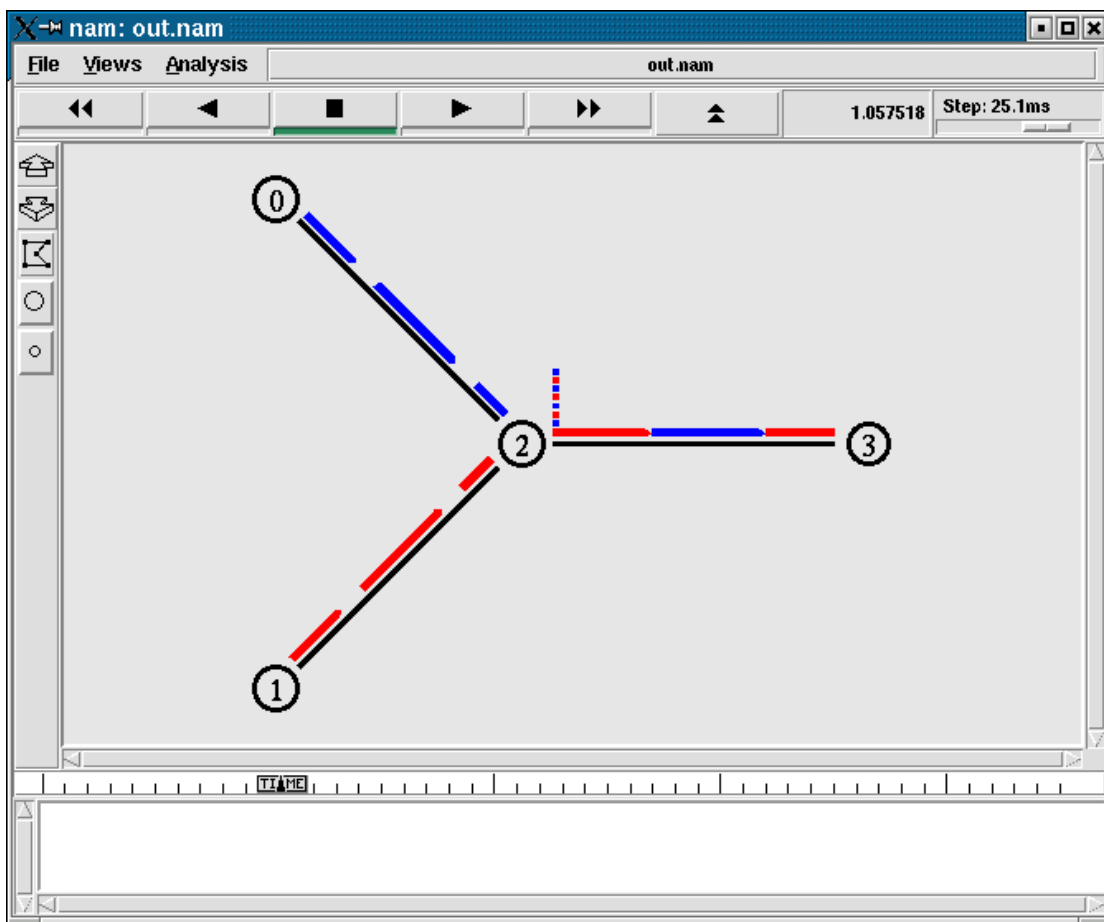


Figure 5.3: Screenshot of the graphical output file of the OTcl code of figure 5.2.

NS2 makes use of the network animator module (NAM) to display the output of a simulation in a graphical form. NAM allows the user to pause, slow down or fast forward through a simulation, as well as zooming in or out to view large topologies. The text box at the bottom of the NAM window gives the user the status of the latest events in the simulation. Apart from this, NAM also shows the status of the data packets that are traveling through the network. The layout of the NAM window is shown in figure 5.4.

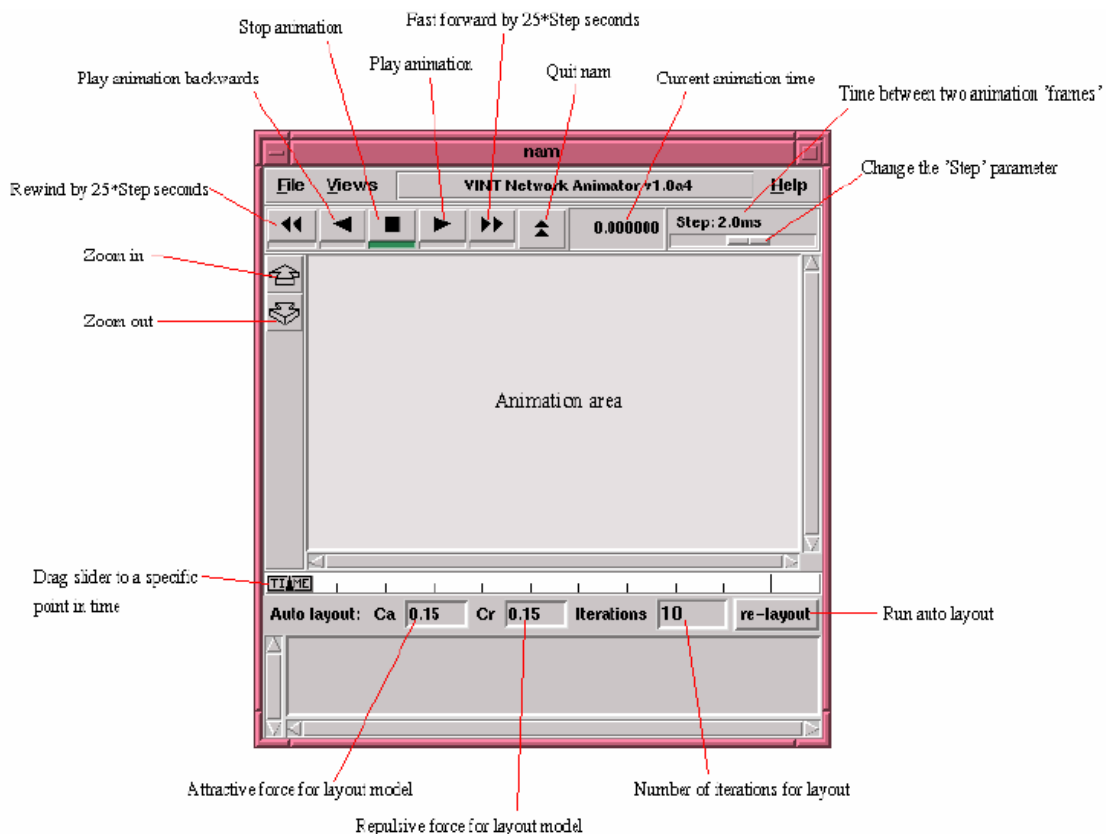


Figure 5.4: Screenshot of the network animator module (NAM) together with descriptions [69].

The biggest drawback of NS2 is the fact that it does not natively support optical WDM networks. WDM network simulations require the use of multiple independent wavelengths per link, and this functionality was lacking in NS2. This shortcoming was remedied by the development of OWns.

### 5.3 OWns

The Optical WDM network simulator (OWns) was developed by the Washington State University to alleviate the shortcomings of NS2 with regard to optical WDM networks. NS2, in conjunction with the OWns extension, is now capable of simulating important aspects of optical fiber communication systems, such as RWA, WDM and optical switching nodes. The network designer is now able to compare the relative performance of different RWA algorithms in different topologies. The package is available for download from the University of Washington [70]. OWns, however, cannot simulate the effects of a link or node failure in a network topology.

OWns also introduces the concept of traffic sessions to simulate the circuit-switched nature of optical networks [71], to compensate for the fact that NS2 has a packet-switched framework at its core. This is due to the fact that optical packet switching, in which the headers of photonic packets (containing IP-addresses, routing information etc.) are read optically, is still many years away [72]. As is shown in figure 5.5, the architecture of OWNS consists of 2 layers: the physical layer and the logical layer. The physical layer consists of the optical nodes and the WDM links, while the logical layer consists of the RWA algorithms and associated routing and wavelength tables.

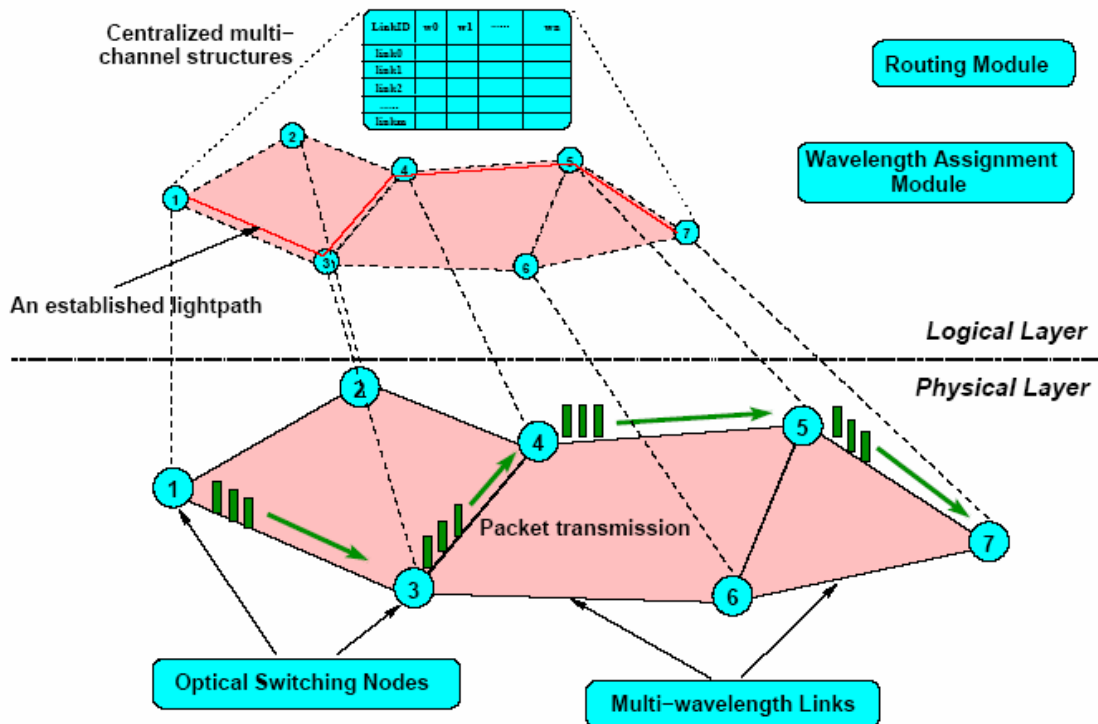


Figure 5.5: OWns architecture and layers [71].

Since the source code of OWns is written in C++, which is an object-oriented programming language, the components of OWns can be organised into objects. The most important of these objects are the following, with their OWns object names given in brackets:

- Optical switching node (WDMNode),
- WDM link (duplex-Fiberlink),
- Routing module (RouteLogic/Wavelength),
- Wavelength assignment module (WAssignLogic).
- Session traffic source objects (Agent/WDM and Application/Session Traffic).
- WDMNode: The WDMNode object is a derivative of the NS Node object, and it consists of a port classifier and a light path classifier. The function of the port classifier is to demultiplex and relay incoming packets to their intended



destinations, which is the `Application/SessionTraffic` object. The function of the light path classifier is to interact with the `WAssignLogic` object in order to establish light paths for incoming traffic sessions, and to issue updates to the state of the virtual topology. At source nodes, a request is issued to the `WAssignLogic` object, while only forwarding information is requested from the object at intermediary nodes. The delay typically introduced in real systems by the wavelength conversion process (if that particular node possesses that capability) is also introduced by the light path classifier, called the `Classifier/Addr/Lightpath` object.

- `duplex-FiberLink`: The `duplex-FiberLink` object is a derivative of the NS `duplex link` object. This new object is able to simulate multiple wavelengths per link, which is the foundation upon which WDM systems are built. It is also possible to modify the per-wavelength bandwidth. A notable change from the NS `duplex link` object is the absence of the queuing component. This difference illustrates the fact that normal electronic traffic can easily be buffered, while the buffering of all-photonics traffic is still at an experimental stage and not commercially viable at present [74].
- `RouteLogic/Wavelength`: The `RouteLogic/Wavelength` object is responsible for the computation and the establishment of the lightpaths needed for the simulation. Since the functionality of the NS routing object and the functionality of the OWns routing object are similar, the OWns `RouteLogic/Wavelength` object is inherited from the NS `RouteLogic` object. The routing information for all the nodes in simulated networks is centrally contained by this object, and the default routing algorithm is the fixed-alternate shortest path algorithm which closely resembles Dijkstra's algorithm (please refer to section 4.2.1). This algorithm determines two paths between each source-destination pair: the shortest path, and another path which is the same length or slightly longer.
- `WAssignLogic`: The `WAssignLogic` object is responsible for wavelength assignment, construction of virtual topologies and the establishment of lightpaths. The `WAssignLogic` interacts closely with the `RouteLogic/Wavelength`

object, and together these two objects are responsible for the RWA of the system. The default wavelength assignment algorithm of OWns is the first-fit algorithm. (please refer to section 4.2.2).

- **Application/SessionTraffic:** The `Application/SessionTraffic` object is responsible for generating traffic at the source nodes of a simulated system. The traffic types that can be simulated include constant bit rate (CBR), exponential and pareto traffic types. Since the NS simulator generates packet traffic while OWns generates circuit-switched session traffic, some modifications have been made. OWns uses three main parameters to specify session traffic, namely mean session arrival rate, mean session holding time and the packet inter-arrival time. The mean session arrival rate is modeled via a Poisson distribution, and the mean session holding time is modeled via an Exponential distribution. The product of these two parameters gives the traffic load measured in Erlangs. The packet inter-arrival time distribution can be chosen to be a CBR, Exponential or Poisson distribution to accurately model different types of traffic sources.

The three available session traffic objects are thus

`Application/SessionTraffic/CBR`,

`Application/SessionTraffic/Exponential` and

`Application/SessionTraffic/Pareto`. Each generated session traffic

object is given a unique flow identification number. When a session starts it

registers with the `WAssignLogic` object, and unregisters when the session ends.

The interaction between the different components in OWns is graphically illustrated in figure 5.6.

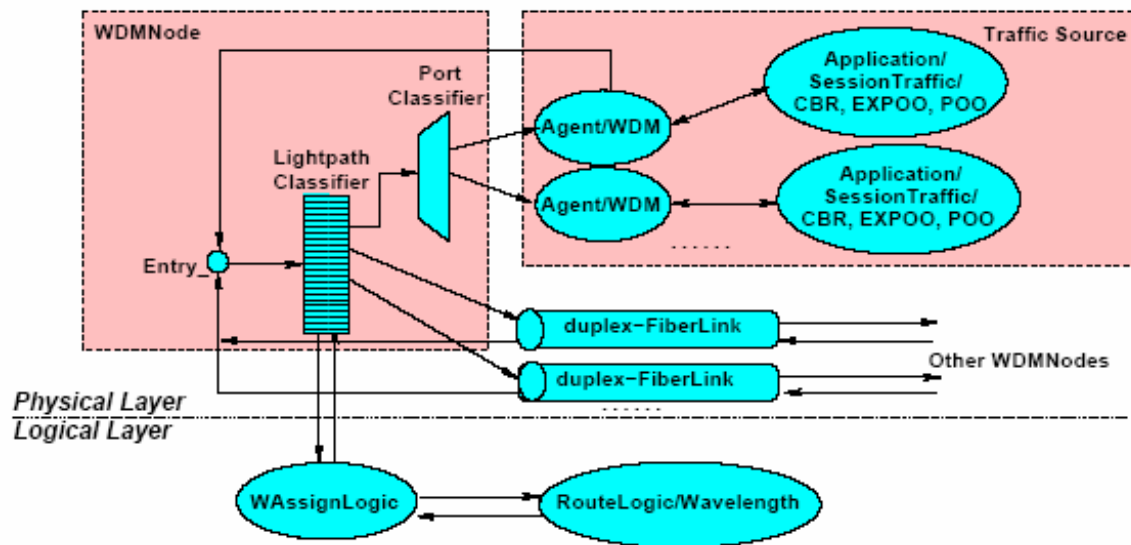


Figure 5.6: OWns components organisation and interactions [71].

# Chapter 6

## Design methodology

The aim of this work is to extend OWns in order for it to be able to simulate protection in optical networks. In order for these results to be verified, it is necessary to test the extended software with some real-world topologies.

### 6.1 Chosen network topologies

It was decided to use three mesh-based topologies that are in use today. These three topologies are:

- The United States backbone network.
- The Italian backbone network.
- The German DFN (*Deutsches Forschungsnetz*, the German Research Network).

In sections 6.1.1 through 6.1.3 the selected topologies are graphically shown, along with their representations in NS2.

#### 6.1.1 The United States backbone network

The US backbone network is a mesh-based network that consists of 28 nodes that are connected by 45 links [57]. This network stretches from coast to coast, connecting most of the major cities. The average connectivity factor of the network is 3.214. This network is graphically shown in figure 6.1, and its NS2 representation is shown in figure 6.2.

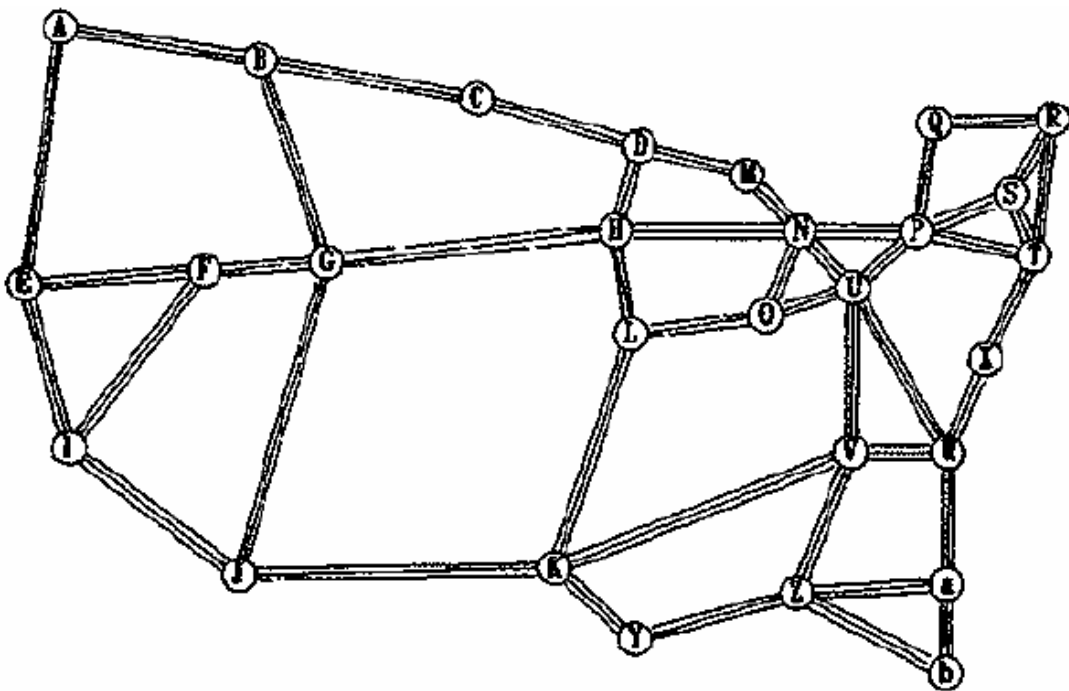


Figure 6.1: The United States backbone network [57].

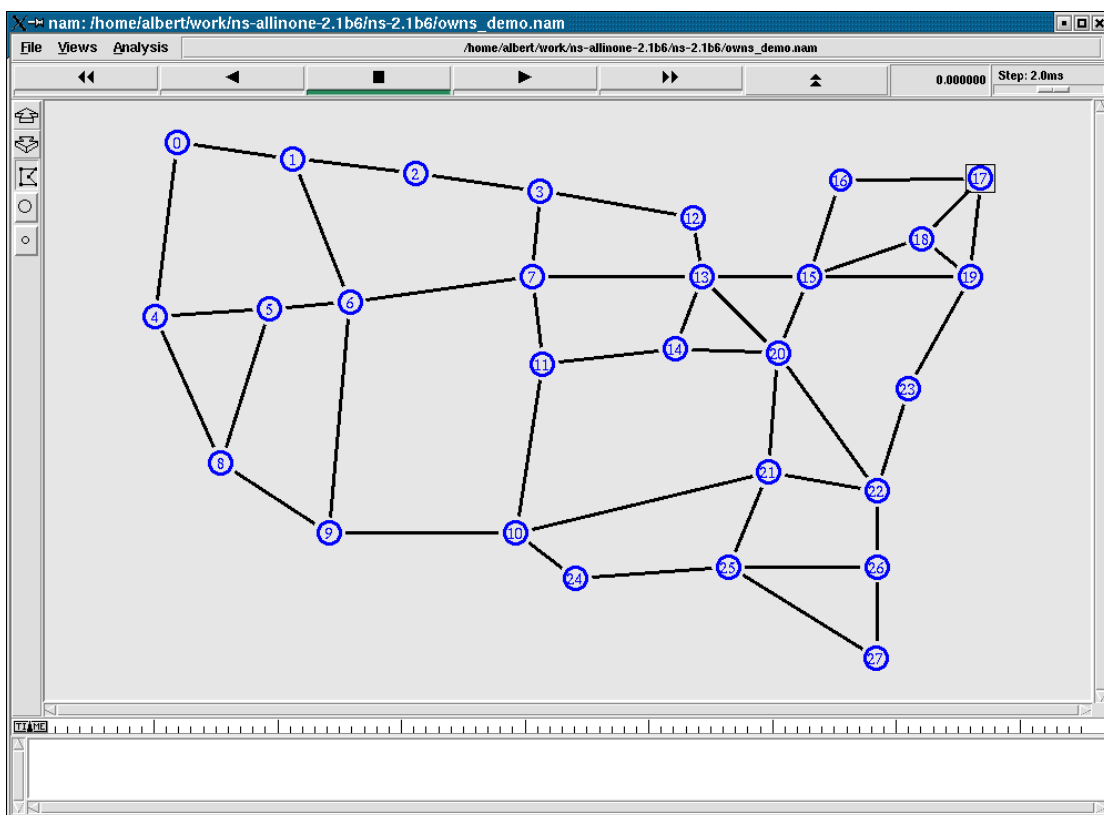


Figure 6.2: Screenshot of the United States backbone network topology created in NS2.

### 6.1.2 The Italian backbone network

The Italian backbone network is a mesh-based network that consists of 21 nodes that are connected by 35 links [73]. This network connects most of the major cities in mainland Italy, as well as connecting cities in Sicily and Sardinia via five undersea cables. The average connectivity factor of the network is 3.428. This network is graphically shown in figure 6.3, and its NS2 representation is shown in figure 6.4.

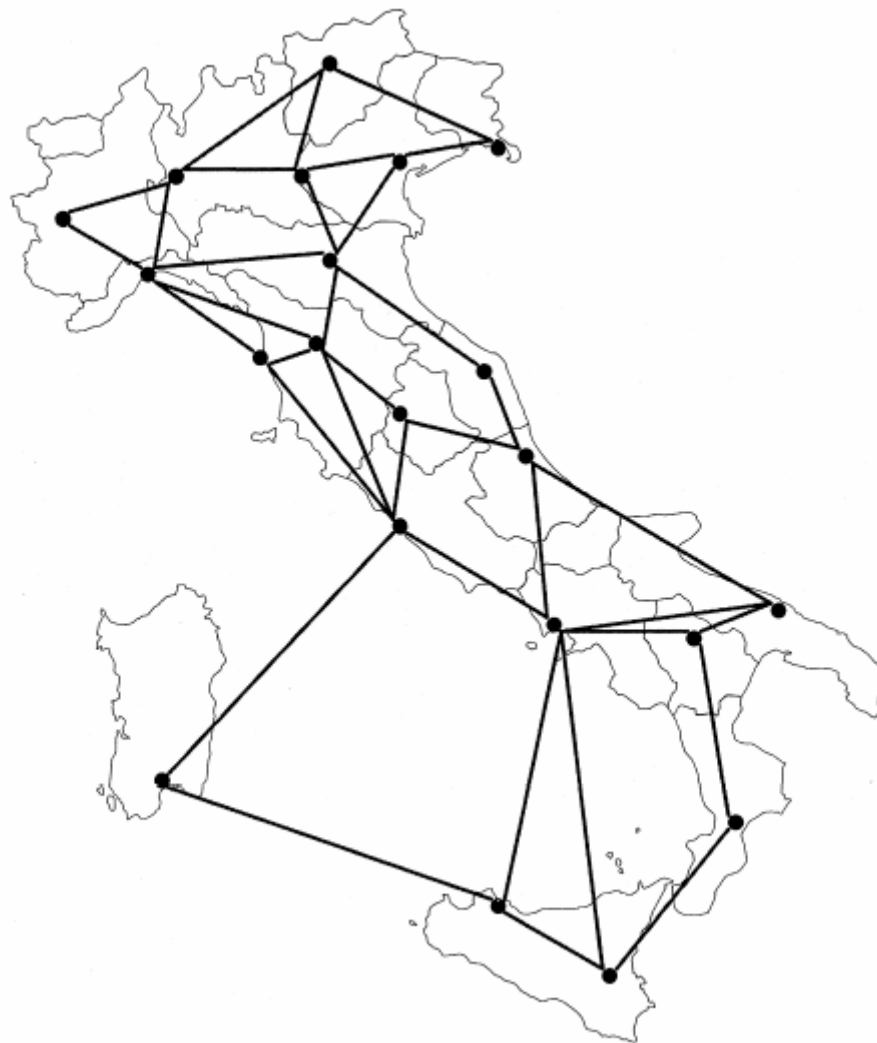


Figure 6.3: The Italian backbone network [73].

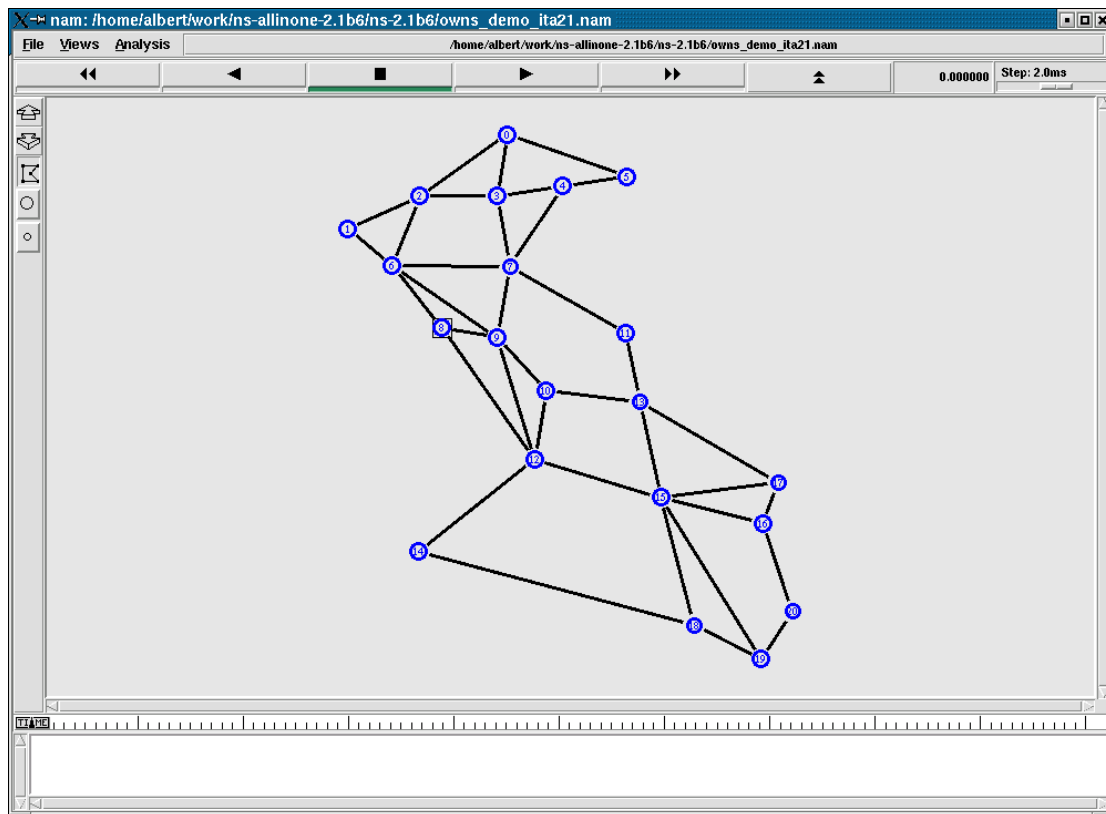


Figure 6.4: Screenshot of the Italian backbone network topology created in NS2.

### 6.1.3 The DFN network

The DFN network is a mesh-based network that consists of 11 nodes that are connected by 23 links. It must be noted that the 11 nodes used only includes those nodes which are connected via 2 or more spatially diverse links: this is due to the fact that nodes that are connected by only one link is totally disconnected from the network if that link is severed. Due to this reason protection and restoration schemes will have no effect, and the simulation results might be influenced adversely. This network provides communication facilities to many German universities as well as private companies and citizens. The average connectivity factor of this network is 4.181.

This network is graphically shown in figure 6.5, and its NS2 representation is shown in figure 6.6, using only the 11 nodes connected by two or more spatially diverse links.

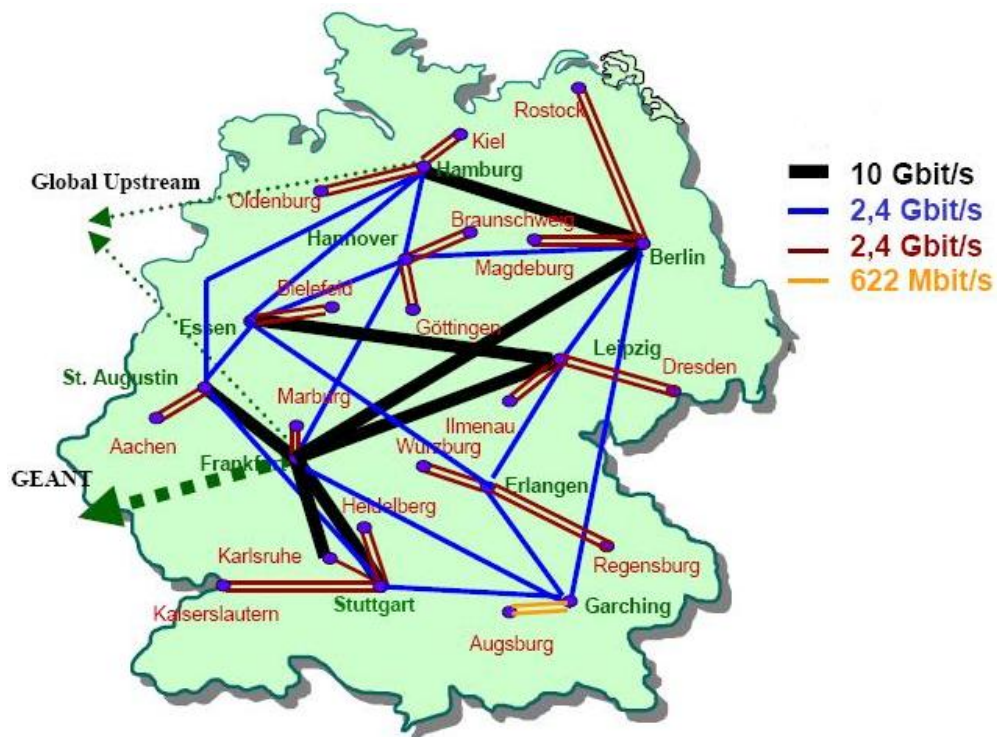


Figure 6.5: Topology of the DFN-network (*Deutsches Forschungsnetz*) [40].

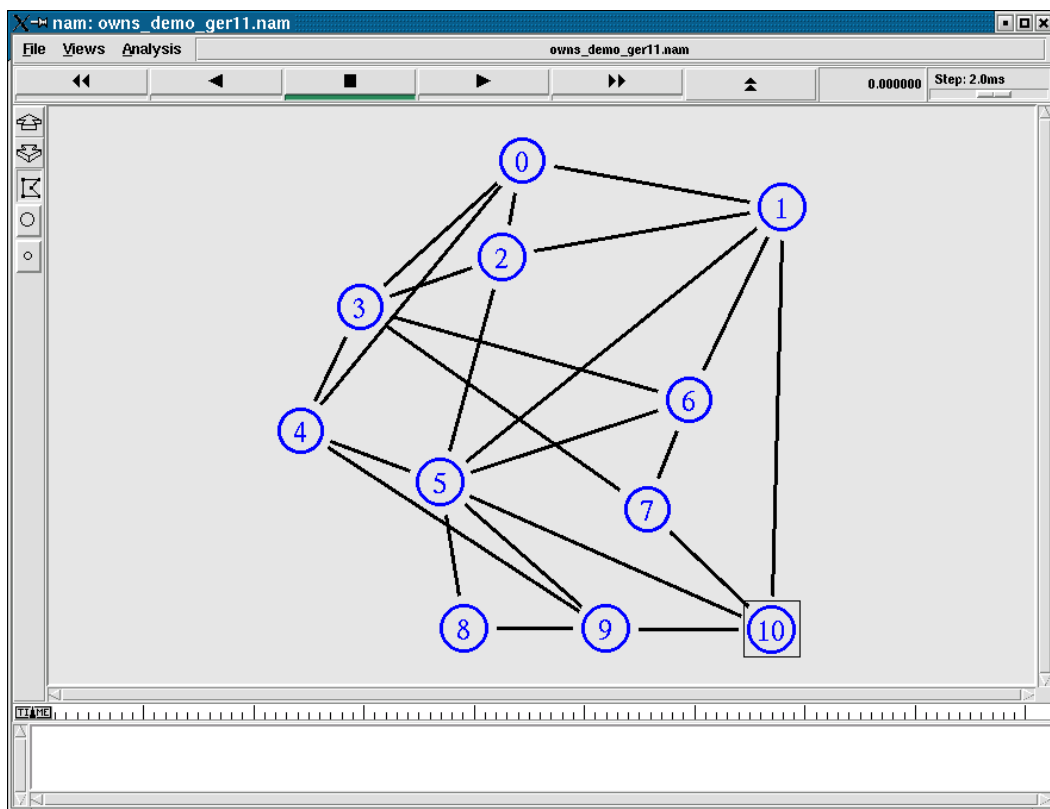


Figure 6.6: Screenshot of the DFN network topology created in NS2.



Table 6.1: Comparison between the United States backbone network, the Italian backbone network and the DFN.

Network name	Nodes	Links	Degree of connectivity
United States	28	45	3.214
Italian	21	35	3.428
DFN	11	23	4.181

## 6.2 Representation of data in NS2 and OWns

### 6.2.1 Graphical presentation of network events and traffic flows

In NS2 data is represented by a stream of data-packets flowing between nodes. OWns modifies this representation, and represents the data-packets of every connection with a different colour. If, for example, there are 8 wavelengths per link, data-packets on a link will be represented by one of 8 different colours.

Note that if data-packets are switched by a node that does not have wavelength conversion capability, the packets that goes into the node and the packets that goes out of the node will always be the same colour, and thus wavelength, for that connection. If the node has wavelength conversion capability, the incoming and outgoing packets might differ in colour (and thus wavelength) if the RWA algorithm determined that a change in wavelength might be beneficial for that particular connection.

A screenshot of this graphical representation of multiple data-packet streams is shown below in figure 6.7, and represents the northwestern corner of the United States backbone network (figure 6.2). In this figure, it can be seen that at least three wavelengths are present in the network, represented by the colours black, orange and green.

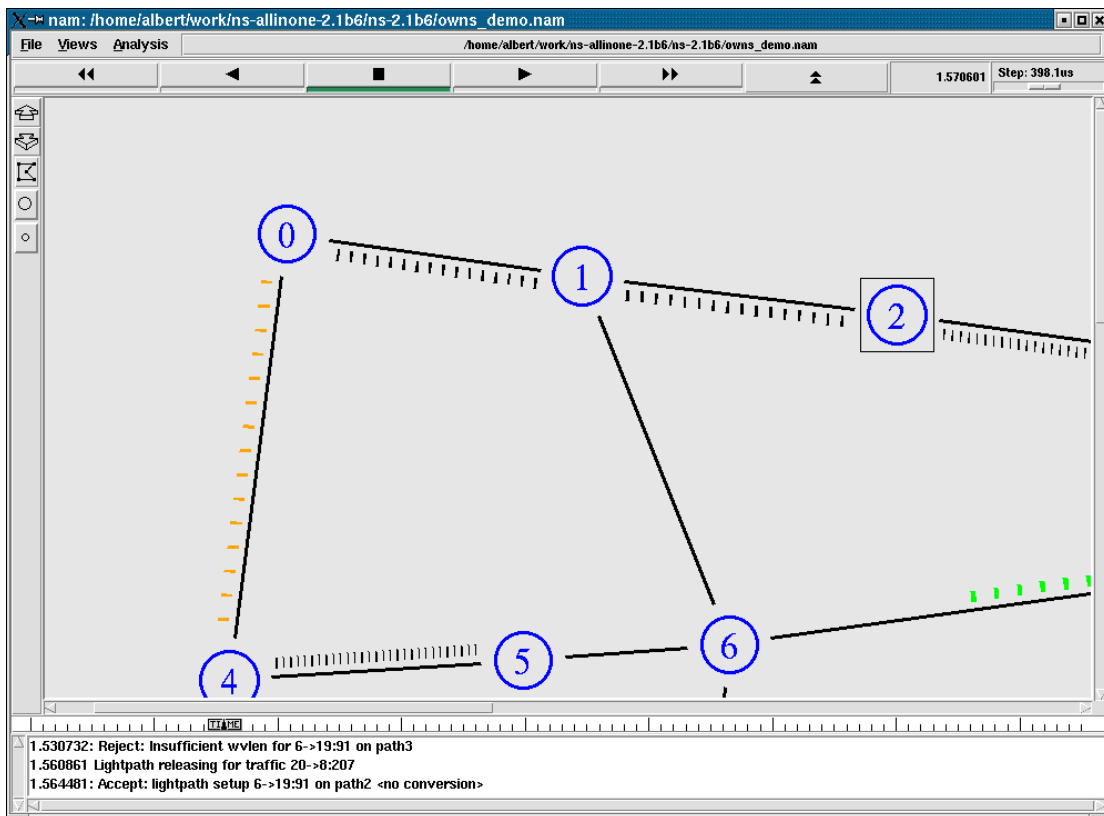


Figure 6.7: Screenshot of OWns, showing different wavelengths represented by different colours.

While the simulation is running, the user can click on individual packets in order to get more information on them. A link is then established to the packet, along with a textbox towards the bottom of the simulation window. The textbox typically contains the source nature of the packet, the size of the packet, the time the packet was sent and the flow identification number of that particular connection.

In figure 6.8, two packets are concurrently being tracked. The packet designated as number 7 comes from an exponential source, has a size of 500 bytes, and was sent 1.215968 seconds into the simulation and makes up part of flow number 52. The packet designated as number 8 also comes from an exponential source, also has a size of 500 bytes, and was sent 1.236650 seconds into the simulation and makes up part of flow number 207.

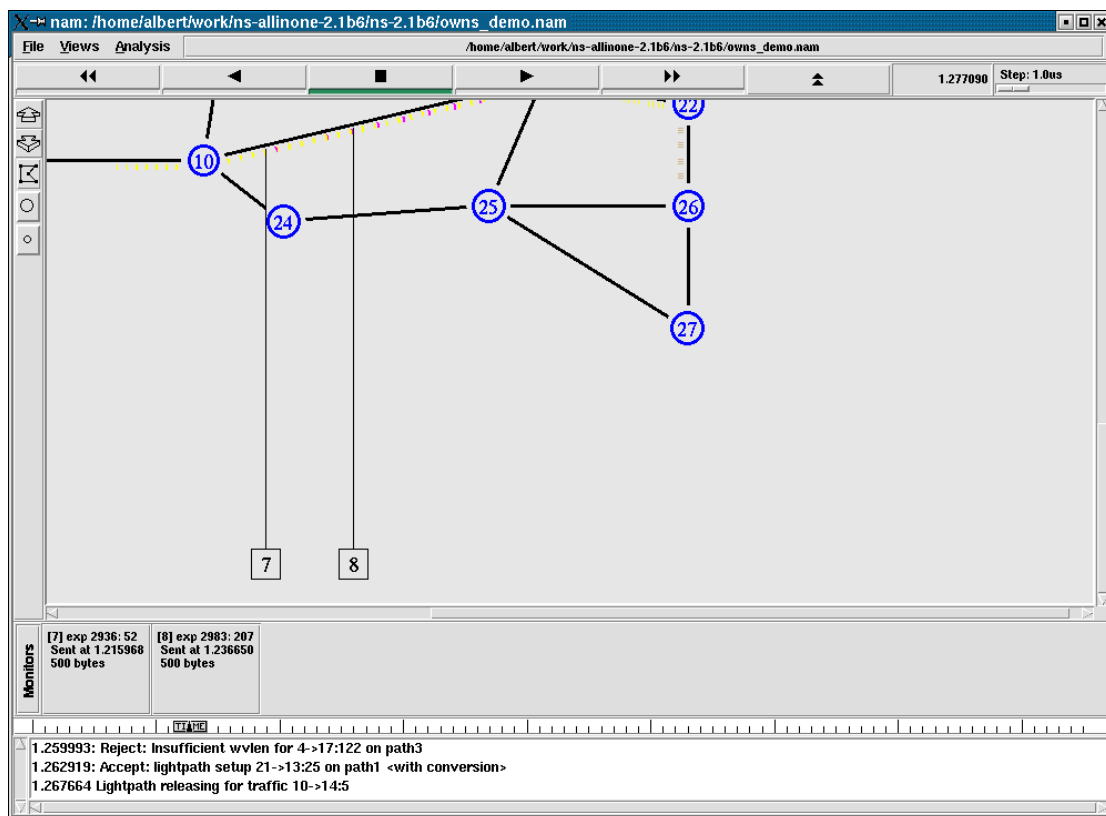


Figure 6.8: Screenshot of OWns, showing two packets that are being tracked, with additional information about the packets being displayed.

The user also has the option of clicking on one of the links itself. If this is done, a graph of the traffic load on that link versus time will be displayed near the bottom of the simulation window. An example of this is shown below in figure 6.9.

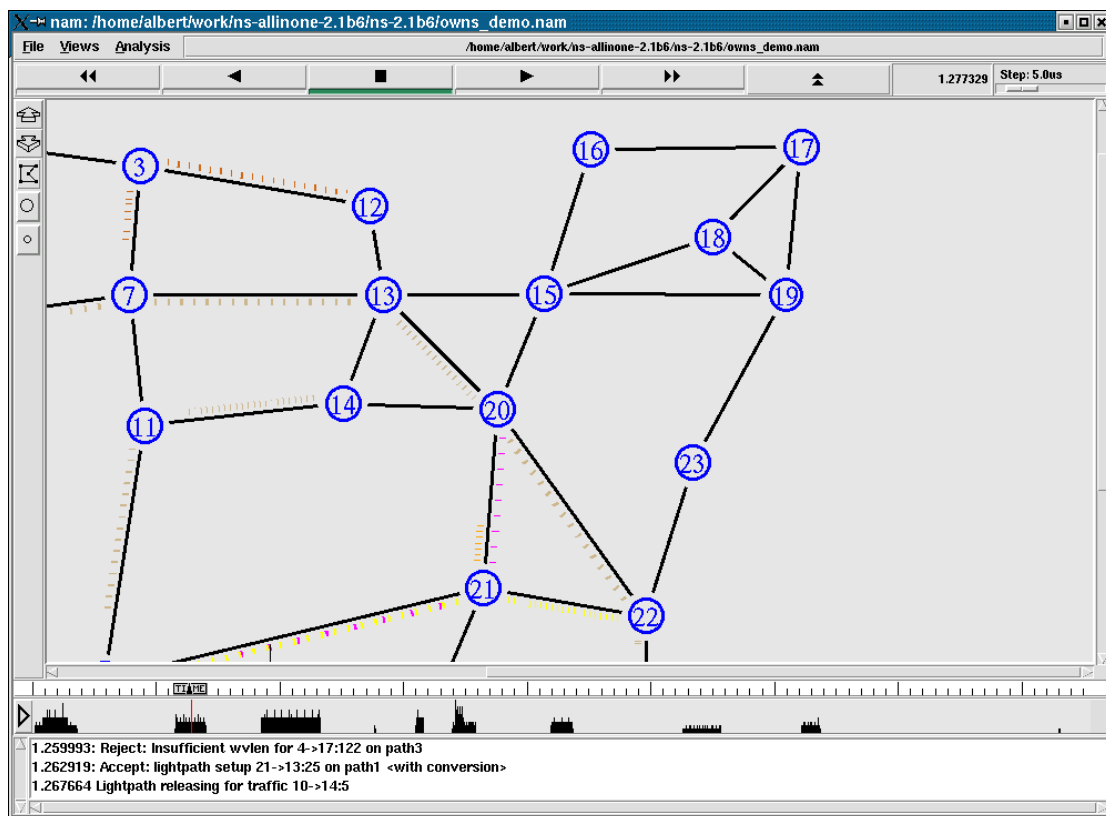


Figure 6.9: Screenshot of OWns, showing the capability of graphically displaying the traffic loads on individual links.

### 6.2.2 Limitations of OWns (excluding restoration and protection)

Currently OWns has some limitations, mostly due to its reliance on the underlying NS2 code. These issues can be resolved by extensive recoding of the NS2 code, but this falls outside the scope of this work. These limitations include:

- All links have the same number of wavelengths per link.
- All wavelengths have the same optical bandwidth.
- Connections are circuit-switched in nature, although they are represented as a stream of packets flowing between the source and destination nodes.
- The same RWA and protection algorithms must be applied to all nodes and links in the network.
- One connection takes up one complete wavelength.
- No queuing of packets can take place at nodes.

### 6.2.3 Tcl file breakdown of OWns

OWns requires the creation of several .Tcl files to configure parameters such as topologies, traffic loads, link failures etc. The figure below, figure 6.10, shows the .Tcl file taxonomy of OWns.

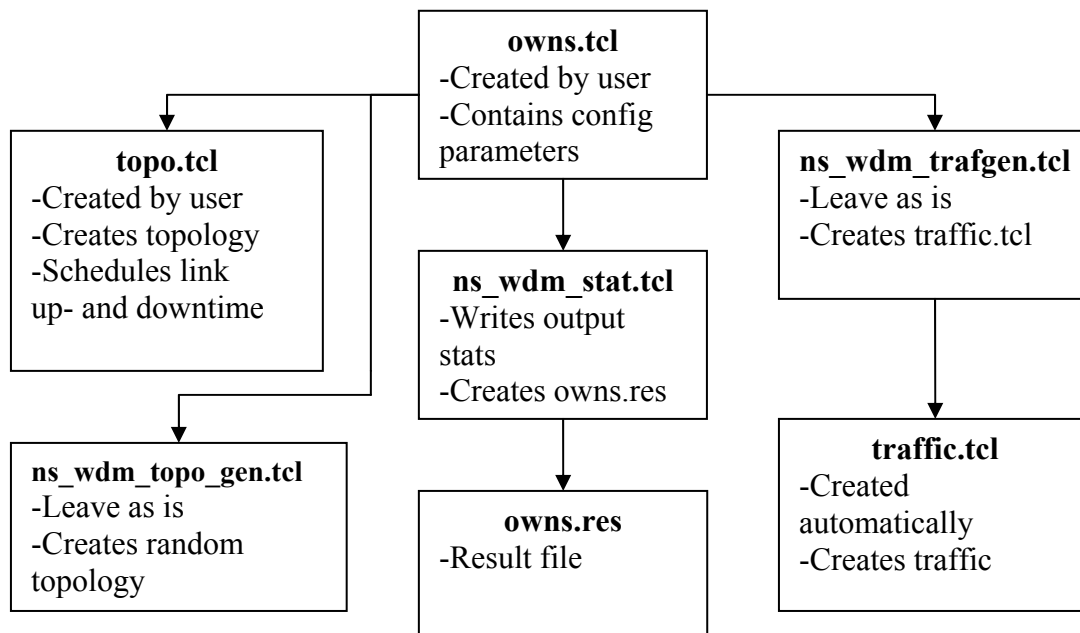


Figure 6.10: The OTcl file taxonomy of OWns.

## 6.3 Design methodology

To do a simulation, the topology needs to be defined first. This is established in the .Tcl configuration script. To establish a topology that contains 28 nodes, the following Tcl code is used:

```

for {set i 0} {$i < 28} {incr i}
{
    set n($i) [$ns $node]
    # create a session-traffic receiver for each node
    set sink($i) [new Agent/$sinker]
    $ns attach-agent $n($i) $sink($i)
}
  
```

Figure 6.11: Tcl code for creation of nodes in network topology.

The segment of Tcl code above creates 28 nodes, labeled from 0 to 27, that are capable of receiving traffic.

Now, the simulation program needs to know which nodes are connected to each other. This is established by using a table with five columns. These columns contain:

- Label of the source node.
- Label of the destination node.
- Time delay between the 2 nodes, in milliseconds.
- Orientation of the destination node relative to the source node.
- Label of the unique link between the source and destination nodes.

```
foreach t {
    {0 1 0.8ms right 0}
    {0 4 0.12ms down 1}
    {4 8 0.8ms down 2}
    {4 5 0.13ms right 3}
    {5 8 0.12ms left-down 4}
    {5 6 0.4ms right 5}
    {8 9 0.14ms right-down 6}
    {6 9 0.14ms down 7}
    {
        ...
    }
}
```

Figure 6.12: Segment of Tcl code (table *t*) illustrating link creation, link delay, link orientation and link identity.

Thus, as can be seen from the figure above, each row of the table contains information specific to a link between two nodes. The third column, in milliseconds, is the propagation delay between two nodes. This propagation delay is directly proportional between the distance between the two nodes, and can be determined by the formula

$$d = (c/1.5) * t \quad (6.1)$$

where *d* is the distance between the two nodes, *c* is the speed of light, 1.5 is the refraction index of a single-mode optical fiber, and *t* is the time delay in seconds. A propagation delay of 0.8 milliseconds thus relates to a distance of 160 km between nodes 0 and 1. Note

that this is the pure propagation delay of the optical signal only and does not include processing and wavelength conversion times at the nodes.

Before the topology can be finalised, it is necessary to finalise the last links. The table  $t$ , shown in figure 6.12, is used as input for the next two steps. The table  $t$  is analysed one row at a time. From each row, the following information is extracted:

- $\$n([lindex \$t 0])$ , column 0, the label of the source node.
- $\$n([lindex \$t 1])$ , column 1, the label of the destination node.
- $[lindex \$t 2]$ , column 2, the propagation delay between the two nodes in milliseconds.
- $[lindex \$t 3]$ , column 3, the orientation of the destination node relative to the source node.
- $[lindex \$t 4]$ , column 4, the unique identification label of that particular link.

Other variables that are also used, are extracted from other configuration files and include:

- $\$linkBW$ , the bandwidth of that particular link.
- $\$wvlens$ , the number of wavelengths that are available on that link.

```
{
$ns duplex-FiberLink $n([lindex $t 0]) $n([lindex $t 1])
    $linkBW [lindex $t 2] Null $wvlens
$ns duplex-link-op $n([lindex $t 0]) $n([lindex $t 1]) orient
    [lindex $t 3]
}
```

Figure 6.13: Segment of Tcl code illustrating logical link creation.

The function `duplex-FiberLink` takes the above information and establishes a duplex (bi-directional) link between the two source nodes in question, including bandwidth and wavelength parameters.

The function `duplex-link-op` takes the information contained in table  $t$  and ensures that the two nodes in question are correctly oriented relative to each other.

## 6.4 Scope of this work

### 6.4.1 Improvements made to OWns

Numerous improvements were made to OWns in order to increase the functionality of the program. The most important of these include:

- The ability to introduce random link failures to any network topology.
- A third path was introduced. Although not crucial, this was brought about to see what benefit, if any, would be achieved by the introduction of a third possible path for any traffic request.
- A protection scheme was implemented that causes the system to recognize a failure in a link, and route affected traffic around this discontinuity.

#### 6.4.1.1 Introduction of random link failures

NS2 contains default commands that can implement link failures, although OWns in its basic form is unable to take advantage of these features. In NS2, normal, functioning links are drawn in black, while non-functional links are drawn in red. An example of these commands is given below, and will cause the link between node 8 (Los Angeles) and node 9 (San Diego) to fail at 0.5 seconds, and the link to come back up at 1.0 seconds.

```
#Link down
$ns rtmodel-at 0.5 down $n(8) $n(9)
#Link up
$ns rtmodel-at 1.0 up $n(8) $n(9)
```

Figure 6.14: Segment of Tcl code illustrating link failure and restoration of service.



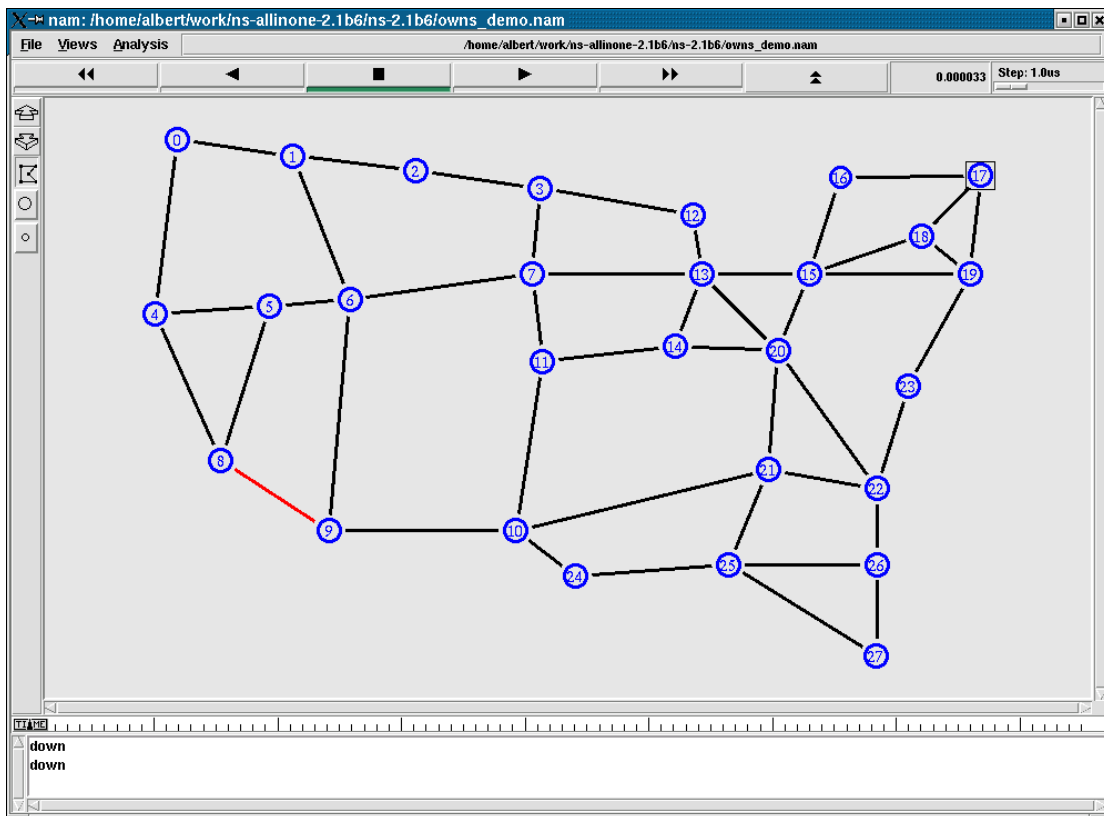


Figure 6.15: Screenshot of OWns, showing link failure between nodes 8 and 9.

However, for a truly realistic simulation scenario, it is necessary to have link failures that take place randomly in a network. In order for this to happen, it is necessary to extract the topology information presented in table  $t$ .

The information we are now interested in is in table  $t$  and is column 0 (source node), column 1 (destination node) and column 4 (link identification number). The user-defined variable `$failurenumber`, signifying the number of link failures during the simulation timeframe, is also needed and is extracted from the user configuration script.

A randomization sequence is initiated, and it selects a number of random link identifier numbers, along with their source and destination nodes, from table  $t$ . The number of links selected is equal to the user-defined variable `$failurenumber`. The extracted list of source and destination nodes are respectively stored in arrays `$sourcelist` and `$destlist` that have a one-to-one mapping with respect to each other.

It is important to note that the randomization sequence must be seeded. The seed can be constant, in which case it will produce a pseudo-random output that gives the same output random sequence every time the program is executed, which is useful for debugging. The seeding can also be derived from other sources e.g. the system clock, in which case the output random sequence will differ every time the program is executed.

Another randomization sequence is used to define random values for variable `$arrivaltemp`. The number of time instances generated is equal to the user-defined variable `$failurenumber`. Variable `$arrivaltemp` defines the time instant when one of the links experiences failure. The figure below illustrates the commands that are used to bring the links down and up. In the figure below the links are brought up 0.5 seconds after they have failed. Please refer to the CD-ROM for the complete source code.

```
For {set j 0} {$j < $failurenumber} {incr j} {
set arrivaltemp [$arrival_ value]
$ns rtmodel-at [expr $arrivaltemp] down $n($sourcelist($j))
           $n($destlist($j))
$ns rtmodel-at [expr $arrivaltemp + 0.5] up $n($sourcelist($j))
           $n($destlist($j))
}
```

Figure 6.16: Segment of Tcl code illustrating randomization of link failures.

A major improvement on studies of similar nature regarding protection and restoration is that NS2, with the implemented OWns extension, is now capable of simulating simultaneous multiple-link failures. Most research up to now has concentrated on optical networks with single-link failures [75]. In figure 6.17 a multiple-link failure is shown, where there are 2 simultaneous links down in the network:

- Link failure between node 2 and node 3.
- Link failure between node 24 and node 25.

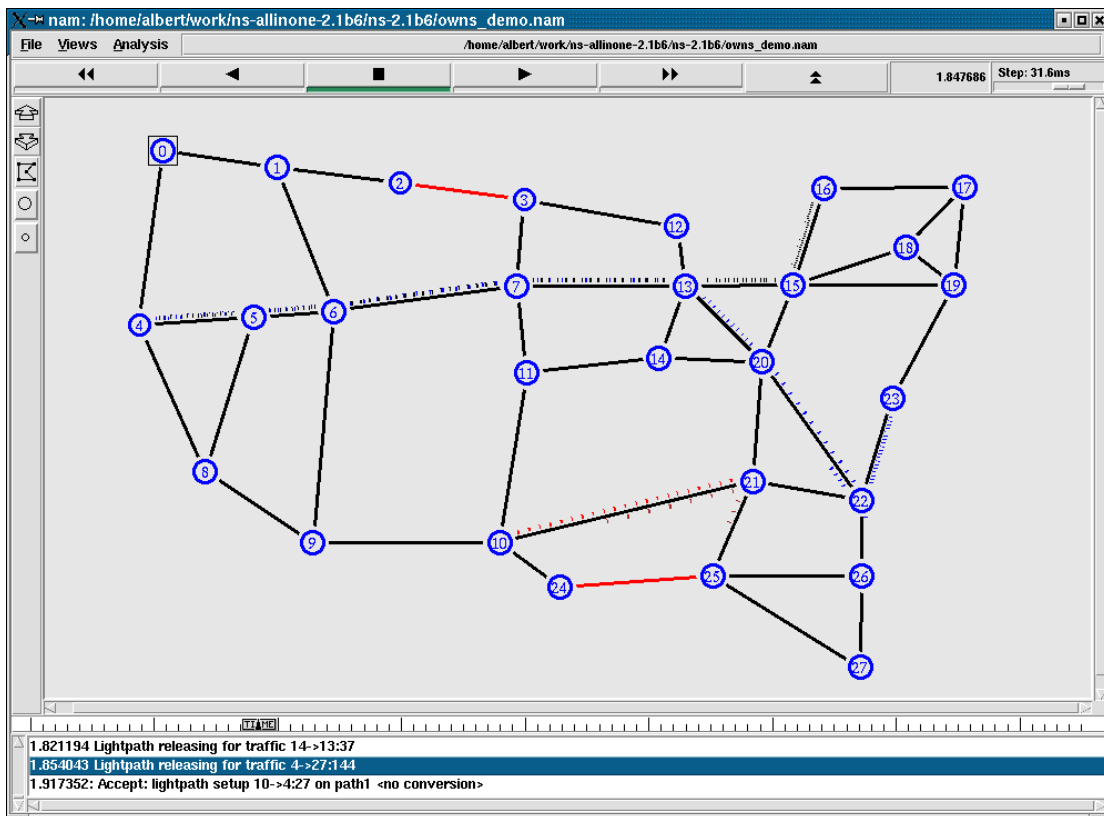


Figure 6.17: Screenshot of OWns, showing 2 links that are down simultaneously.

#### 6.4.1.2 Introduction of a third path

In its original form, NS2 and OWns calculates two possible paths for every traffic request. This consists of the shortest path, utilising Dijkstra's algorithm (path 1), and an alternate path (path 2), as short as possible, that tries to be disjoint from the first path. Traffic will always try to use path 1, and only when no capacity is present on path 1, will the traffic be allocated to path 2.

A third path was implemented in this implementation of OWns to try to determine what benefits a third path will bring, especially with respect to blocking probability. Blocking probability is defined as the percentage of total connections that is unable to be completed due to capacity constraints or link failures.

The third path was implemented by giving all possible links in the topology a random weight (after the first two paths per connection were determined). The route with the lowest weight was deemed to be the third route. The reason for the choice of the shortest

random path was due to the fact that the shortest path and the shortest disjoint path have already been allocated. This third route will typically use segments of path 1 and path 2, as well as segments unused by paths 1 and 2. The reason why a totally disjoint third path wasn't implemented stems from the fact that a third disjoint route does not always exist, especially in routes close to the edge of a network. In addition to this, in networks of low connectivity, finding a third path, disjoint from paths 1 and 2, might turn out to be more than twice as long as the shortest route. A third, disjoint route of this nature, causes more capacity constraints than it solves.

Extensive additional coding of OWns as well as NS2 was required to implement the third path in the simulation scenarios. Full source code can be found on the CDROM.

#### **6.4.1.3 Introduction of a protection scheme to OWns**

As of present, protection has not yet been implemented in OWns. Thus, the most important and novel contribution by this author to OWns is the introduction of a strategy and associated algorithms to reroute traffic around failed links in an optical network.

The implemented protection scheme is in the form of a centrally controlled protection scheme. This is a protection scheme, and not a restoration scheme. This implies that a set of finite paths for each traffic connection is established beforehand, in contrast to a restoration scheme where a new route is dynamically determined after a failure has occurred. The main advantage protection has above restoration is the reduced time in switching traffic from the broken path to the new backup path. The implementation for a restoration scheme is left as a future contribution.

The steps the protection scheme takes must be seen in conjunction with the RWA of the program. In combination, these are:

- Numerous traffic flows are defined per simulation. For example, one of these can be source node 0 to destination node 11.

- Path 1 is determined. This is calculated using Dijkstra's open shortest path first (OSPF) algorithm. In the US backbone network (figure 6.2) this path would be 0-4-5-6-7-11.
- Path 2 is determined. This path is the shortest path that is disjoint to path 1. In the US backbone network, this would be 0-1-2-3-7-11.
- Path 3 is determined. Weights are randomly allocated to links between nodes in the network, with the path being chosen having the shortest combined weight of all possible variations. In the US backbone network, one possibility for path 3 would be 0-4-5-6-9-10-11.
- Wavelength assignment is done using the first-fit algorithm, i.e. the first open wavelength on a link is always assigned to a traffic request. The reason for the choice of the first-fit algorithm is its superior performance compared to other algorithms (if utilisation of computational resources is taken into account) [51].
- When faced with a traffic request, the routing assignment algorithm always tries to use path 1 first. If unable to allocate path 1, path 2 is allocated to that particular traffic request. If unable to allocate path 2, path 3 is allocated to that particular traffic request. If unable to allocate path 3, the blocking probability counter is incremented.
- When the simulation is running and the protection algorithm senses the presence of a broken link that causes a traffic flow to drop packets, the traffic flow is:
  - Redirected to path 2 or path 3 (if the traffic flow was on path 1).
  - Redirected to path 3 (if the traffic flow was on path 2).
  - If unable to redirect the traffic flow due to inadequate network resources, the blocking counter is incremented.

A flow diagram of this process can be seen on the next page as figure 6.18.

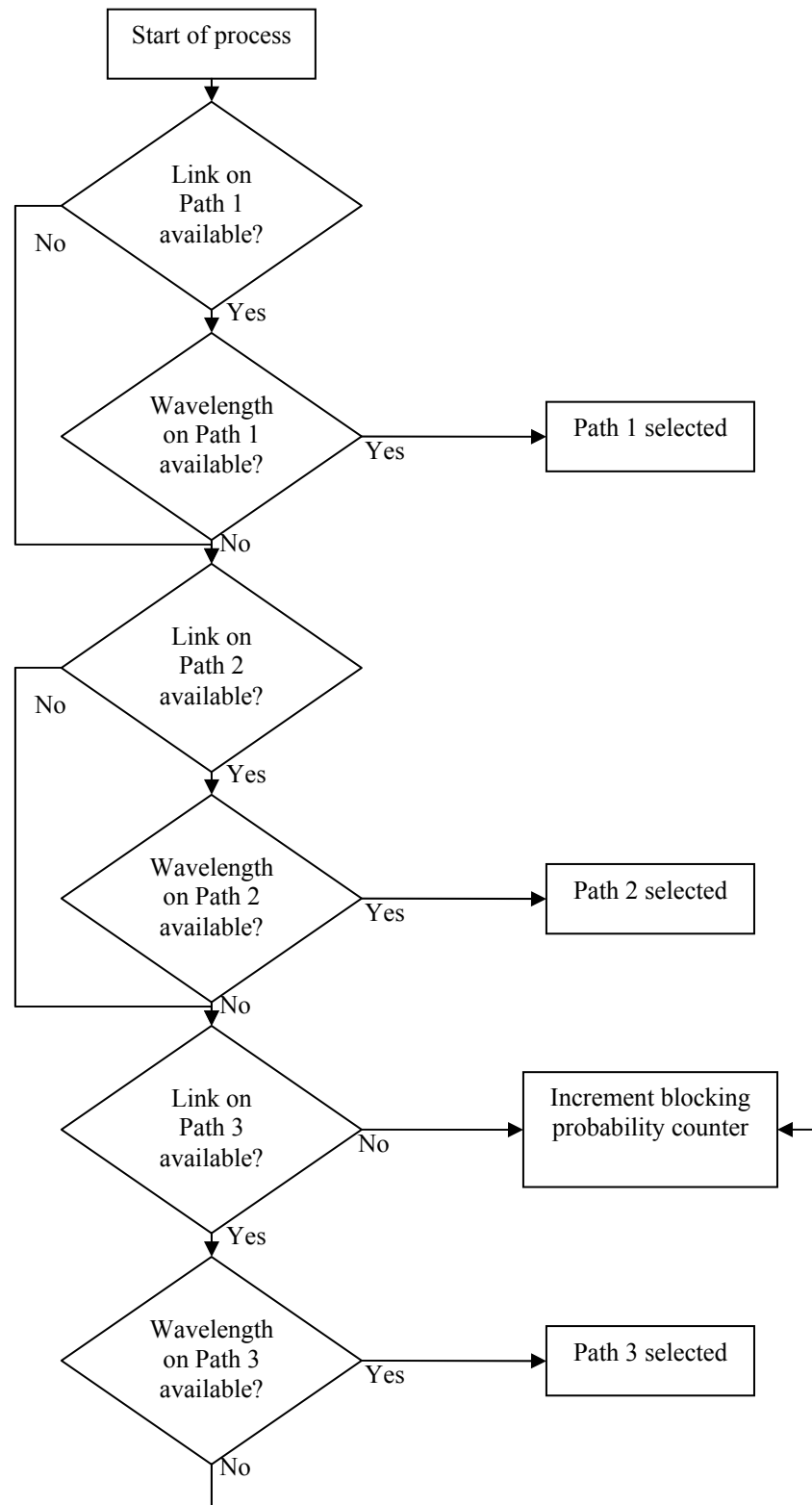


Figure 6.18: Flowchart of the modified path selection and new protection strategy in OWns.

Extensive recoding as well as the addition of new software modules and code for OWns as well as NS2 was required to implement the protection functionality. Full source code can be found on the CDROM.

#### 6.4.2 Description of simulation scenarios

The three topologies described earlier in this work, namely the United States backbone network (figure 6.2), the Italian backbone network (figure 6.4), and the *Deutches Forschungsnetz* (figure 6.6) will be simulated to determine the results.

Factors that will determine the results are the following:

- Degree of connectivity.
- Number of wavelengths per link.
- Number of traffic flows per network.
- Number of link failures per network.

The United States backbone network was taken as the reference network. Due to differences in connectivity, the traffic flows per network and the link failures per network for the Italian and DFN networks have been normalised with respect to the United States backbone network. This has the end result of having all networks compete on a level footing – all have the same amount of wavelengths, traffic flows and link failures per link.

It proved impossible to normalize the simulation parameters of the Italian and DFN networks perfectly with the Unites States network. This is due to the need to deal with integer numbers with certain parameters – i.e. 58 traffic flows per network is allowed, while 58.1 will not be allowed. The simulation parameters are shown in tables 6.2-6.4 – thus forming a total of 360 different simulation scenarios (4 different wavelengths \* 6 different link failures \* 5 different number of traffic sessions \* 3 topologies). Each of these 360 scenarios was run a total of 5 times each.

Common simulation parameters for all scenarios include:

- All nodes have wavelength conversion capability (for an extensive review of OWns and wavelength conversion capability results, please see [71]).
- All links have the same number of wavelengths.
- All wavelengths have the same bandwidth.
- NS2's standard routing, namely OSPF, is used with the addition of the third path.
- The first-fit wavelength assignment is used.
- All traffic sources are exponential traffic sources.
- The protection scheme is implemented.

Table 6.2: Network simulation topology parameters – wavelengths.

	<b>Nodes</b>	<b>Links</b>	<b>Connectivity</b>	$\lambda$
<b>US</b>	28	45	3.214	2
				4
				8
				16
<b>ITA</b>	21	35	3.428	2
				4
				8
				16
<b>DFN</b>	11	23	4.181	2
				4
				8
				16



Table 6.3: Network simulation topology parameters – link failures.

	<b>Nodes</b>	<b>Links</b>	<b>Connec- tivity</b>	<b>Link failures (normalised)</b>	<b>Link failures chosen (% error relative to reference)</b>
<b>US</b>	28	45	3.214	0	0 (0%)
				2	2 (0%)
				4	4 (0%)
				6	6 (0%)
				8	8 (0%)
				10	10 (0%)
<b>ITA</b>	21	35	3.428	0.0	0 (0%)
				1.6	2 (+25%)
				3.2	3 (-6.25%)
				4.8	5 (+4.16%)
				6.4	6 (-6.25%)
				8.0	8 (0%)
<b>DFN</b>	11	23	4.181	0.0	0 (0%)
				1.03	1 (-3%)
				2.06	2 (-3%)
				3.09	3 (-3%)
				4.12	4 (-3%)
				5.15	5 (-3%)

Table 6.4: Network simulation topology parameters – traffic sessions.

	<b>Nodes</b>	<b>Links</b>	<b>Connec- tivity</b>	<b>Traffic sessions (normalised)</b>	<b>Traffic sessions chosen (% error relative to reference)</b>
<b>US</b>	28	45	3.214	15	15 (0%)
				30	30 (0%)
				45	45 (0%)
				60	60 (0%)
				75	75 (0%)
<b>ITA</b>	21	35	3.428	11.6	12 (+3.44%)
				23.2	23 (-0.86%)
				34.8	35 (+0.57%)
				46.4	46 (-0.86%)
				58.0	58 (0%)
<b>DFN</b>	11	23	4.181	7.6	8 (+5.26%)
				15.2	15 (-1.31%)
				22.8	23 (+0.87%)
				30.4	30 (-1.31%)
				38.0	4 (0%)

# Chapter 7

## Results

The results obtained follow in the following sections. Selected results are shown in tabular as well as graphical form. The complete results for all 360 scenarios can be found in Appendix A.

### 7.1 Blocking probability

Blocking probability is defined as the fraction of attempted connections that are unable to be completed due to insufficient network resources. In figures 7.1 through 7.9, results are graphically given for some of the various simulation scenarios. Following is a summary of the results regarding blocking probabilities.

The blocking probability increases as the traffic increases. This intuitive idea is reflected in the simulation results. In general, topologies with higher connectivity factors had lower blocking probabilities than topologies with lower connectivity factors.

The blocking probability increases as the link failures increase. Once again, topologies with higher connectivity factors had lower blocking probabilities (i.e. increased performance) than topologies with lower connectivity factors.

Figure 7.10 shows the average overall blocking probability for all 360 simulation scenarios, with increasing number of wavelengths. It reflects that, generally, mesh topologies with higher connectivities perform better than topologies with lower connectivities over a broad range of available wavelengths and / or link failure scenarios. This graph is smoother than the previous figures, due to the increase of data points.

Table 7.1: Blocking probability with 2 wavelengths and zero link failures.

<b>Blocking probability, 2 wavelengths, zero link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	0	15	0
	0	30	0.027
	0	45	0.181
	0	60	0.108
	0	75	0.230
<b>ITA</b>	0	12	0
	0	23	0.04
	0	35	0.021
	0	46	0.147
	0	58	0.164
<b>DFN</b>	0	8	0
	0	15	0
	0	23	0
	0	30	0.04
	0	38	0

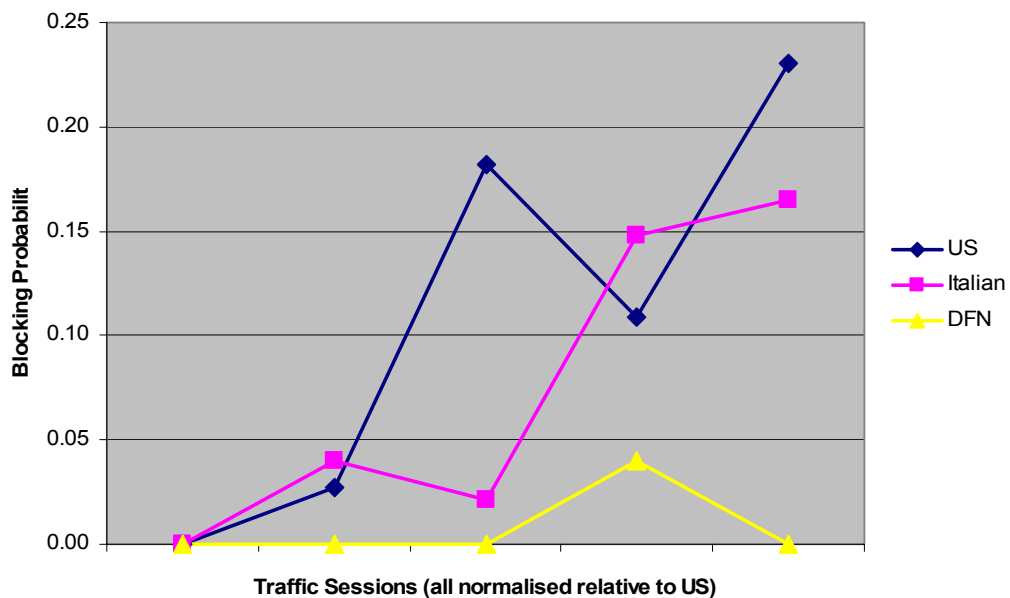
**Blocking Probability, 2 Wavelengths, 0 Link Failures**

Figure 7.1: Blocking probability with 2 wavelengths and zero link failures.

Table 7.2: Blocking probability with 2 wavelengths and moderate number of link failures.

<b>Blocking probability, 2 wavelengths, moderate number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	6	15	0.043
	6	30	0.1
	6	45	0.2
	6	60	0.191
	6	75	0.272
<b>ITA</b>	5	12	0
	5	23	0.04
	5	35	0.115
	5	46	0.220
	5	58	0.168
<b>DFN</b>	3	8	0
	3	15	0
	3	23	0.023
	3	30	0.078
	3	38	0.043

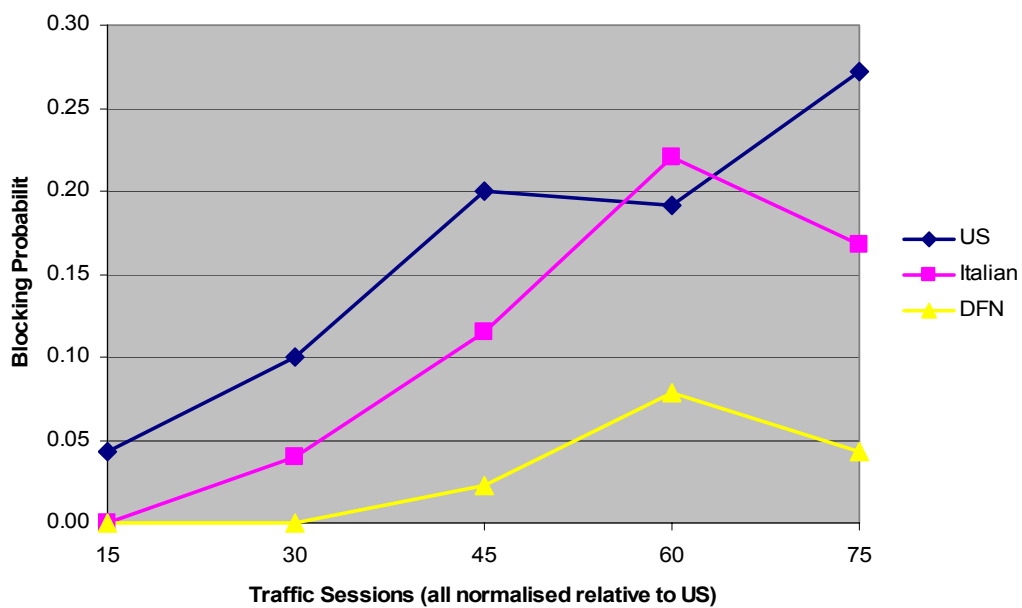
**Blocking Probability, 2 Wavelengths, Moderate Number of Link Failures**

Figure 7.2: Blocking probability with 2 wavelengths and moderate number of link failures.

Table 7.3: Blocking probability with 2 wavelengths and high number of link failures.

<b>Blocking probability, 2 wavelengths, high number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	10	15	0.193
	10	30	0.216
	10	45	0.25
	10	60	0.229
	10	75	0.273
<b>ITA</b>	8	12	0.052
	8	23	0.038
	8	35	0.057
	8	46	0.193
	8	58	0.260
<b>DFN</b>	5	8	0.016
	5	15	0
	5	23	0
	5	30	0.04
	5	38	0

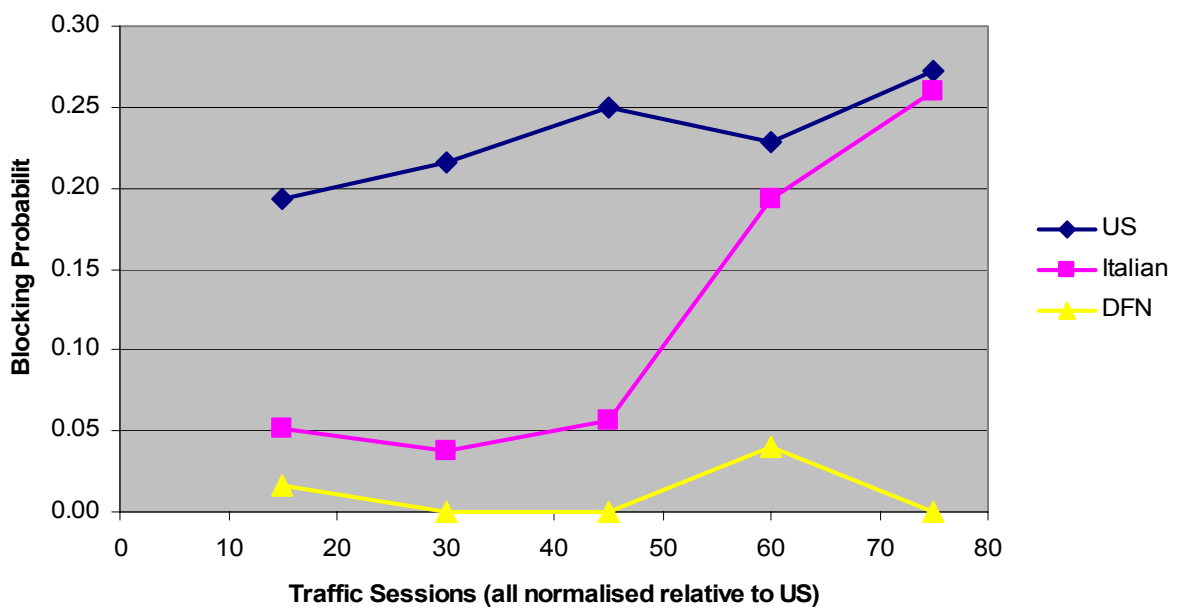
**Blocking Probability, 2 Wavelengths, High Number of Link Failures**

Figure 7.3: Blocking probability with 2 wavelengths and high number of link failures.

Table 7.4: Blocking probability with 4 wavelengths and zero link failures.

<b>Blocking probability, 4 wavelengths, zero link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	0	15	0
	0	30	0
	0	45	0
	0	60	0
	0	75	0.01
<b>ITA</b>	0	12	0
	0	23	0
	0	35	0
	0	46	0
	0	58	0.014
<b>DFN</b>	0	8	0
	0	15	0
	0	23	0
	0	30	0
	0	38	0

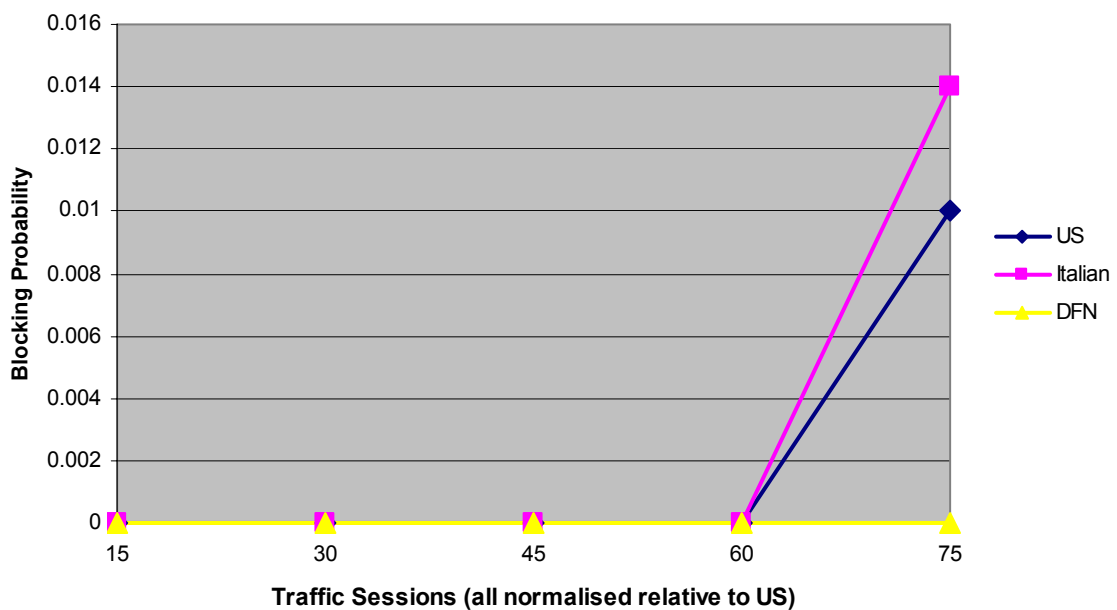
**Blocking Probability, 4 Wavelengths, 0 Link Failures**

Figure 7.4: Blocking probability with 4 wavelengths and zero link failures.

Table 7.5: Blocking probability with 4 wavelengths and moderate number of link failures.

<b>Blocking probability, 4 wavelengths, moderate number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	6	15	0
	6	30	0.01
	6	45	0.012
	6	60	0
	6	75	0.057
<b>ITA</b>	5	12	0
	5	23	0
	5	35	0
	5	46	0
	5	58	0.061
<b>DFN</b>	3	8	0
	3	15	0.021
	3	23	0
	3	30	0
	3	38	0.021

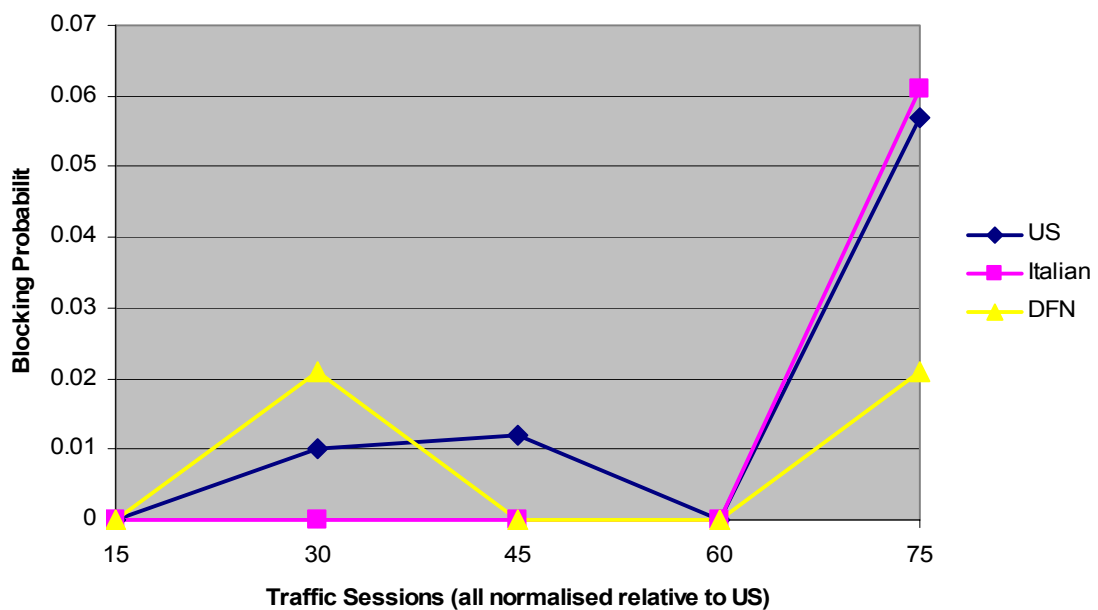
**Blocking Probability, 4 Wavelengths, Moderate Number of Link Failures**

Figure 7.5: Blocking probability with 4 wavelengths and moderate number of link failures.



Table 7.6: Blocking probability with 4 wavelengths and high number of link failures.

<b>Blocking probability, 4 wavelengths, high number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	10	15	0.023
	10	30	0.045
	10	45	0.057
	10	60	0.107
	10	75	0.02
<b>ITA</b>	8	12	0.074
	8	23	0
	8	35	0
	8	46	0.064
	8	58	0.074
<b>DFN</b>	5	8	0
	5	15	0
	5	23	0.021
	5	30	0
	5	38	0.078

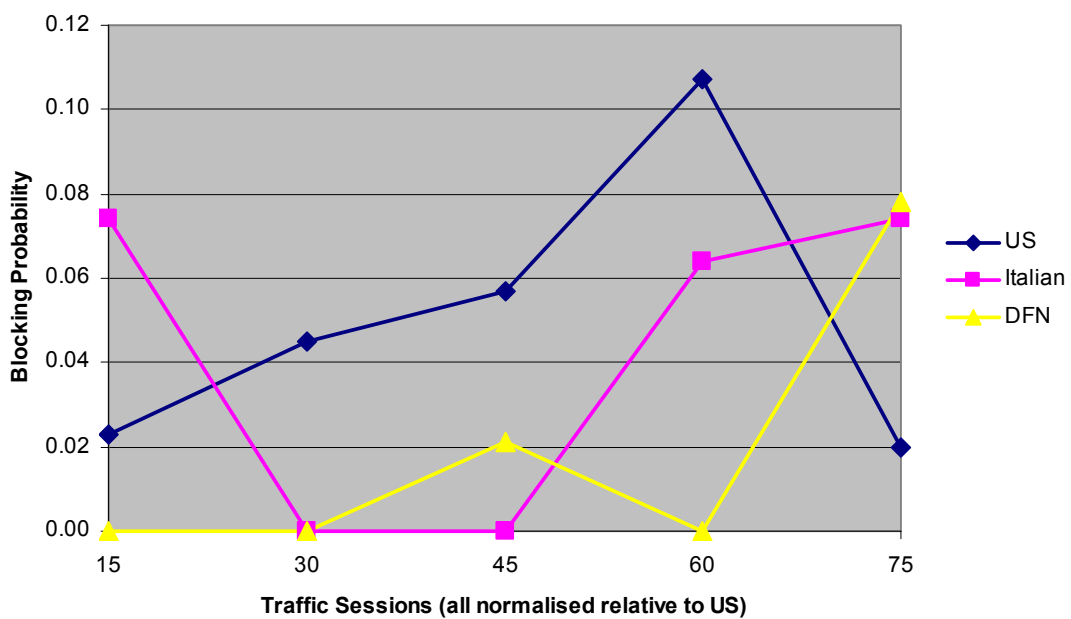
**Blocking Probability, 4 Wavelengths, High Number of Link Failures**

Figure 7.6: Blocking probability with 4 wavelengths and high number of link failures.

Table 7.7: Blocking probability with 16 wavelengths and zero link failures.

<b>Blocking probability, 16 wavelengths, zero link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	0	15	0
	0	30	0
	0	45	0
	0	60	0
	0	75	0
<b>ITA</b>	0	12	0
	0	23	0
	0	35	0
	0	46	0
	0	58	0
<b>DFN</b>	0	8	0
	0	15	0
	0	23	0
	0	30	0
	0	38	0

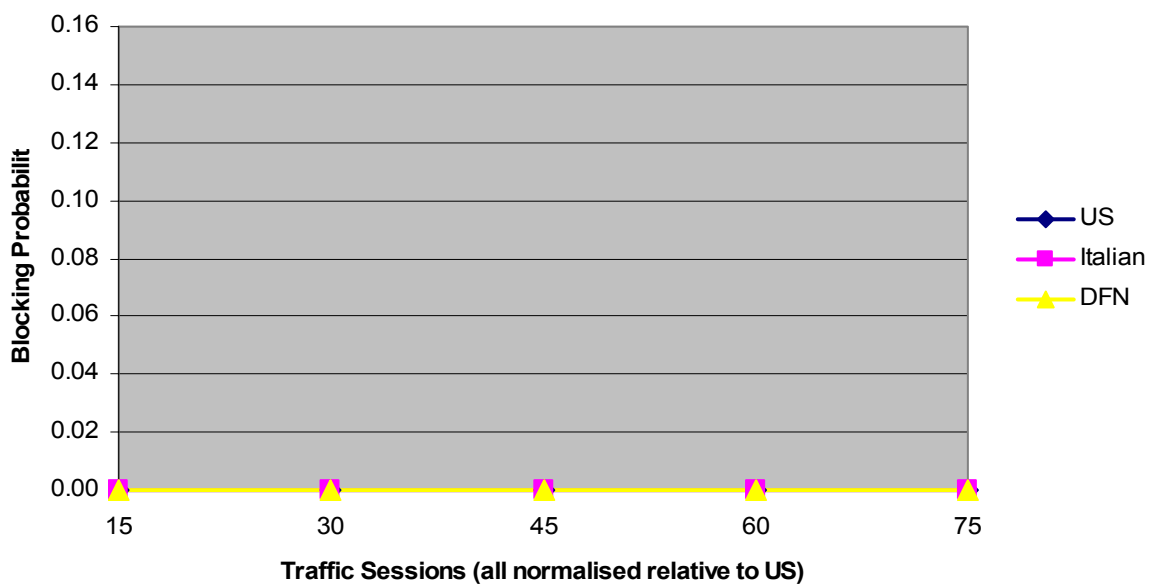
**Blocking Probability, 16 Wavelengths, 0 Link Failures**

Figure 7.7: Blocking probability with 16 wavelengths and zero link failures.

Table 7.8: Blocking probability with 16 wavelengths and moderate number of link failures.

<b>Blocking probability, 16 wavelengths, moderate number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	6	15	0
	6	30	0
	6	45	0
	6	60	0.043
	6	75	0.023
<b>ITA</b>	5	12	0.044
	5	23	0
	5	35	0
	5	46	0.042
	5	58	0
<b>DFN</b>	3	8	0
	3	15	0
	3	23	0
	3	30	0
	3	38	0.02

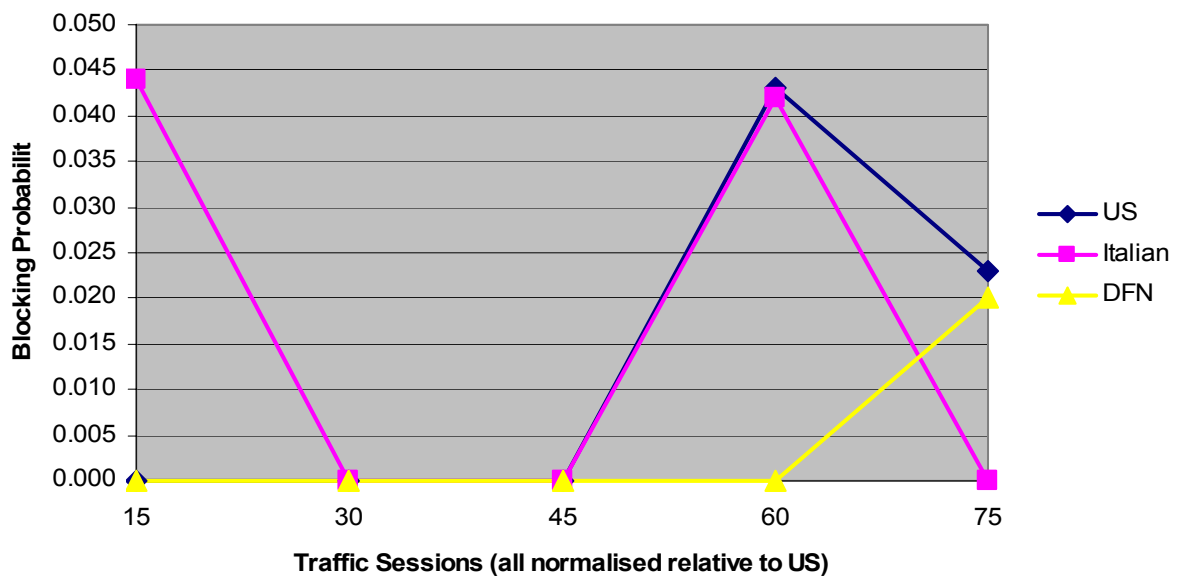
**Blocking Probability, 16 Wavelengths, Moderate Number of Link Failures**

Figure 7.8: Blocking probability with 16 wavelengths and moderate number of link failures.

Table 7.9: Blocking probability with 16 wavelengths and high number of link failures.

<b>Blocking probability, 16 wavelengths, high number of link failures</b>			
	<b>Link Failures</b>	<b>Traffic Sessions</b>	<b>Blocking Probability</b>
<b>US</b>	10	15	0
	10	30	0
	10	45	0.105
	10	60	0.085
	10	75	0.009
<b>ITA</b>	8	12	0.057
	8	23	0
	8	35	0.074
	8	46	0.067
	8	58	0.086
<b>DFN</b>	5	8	0
	5	15	0
	5	23	0
	5	30	0
	5	38	0

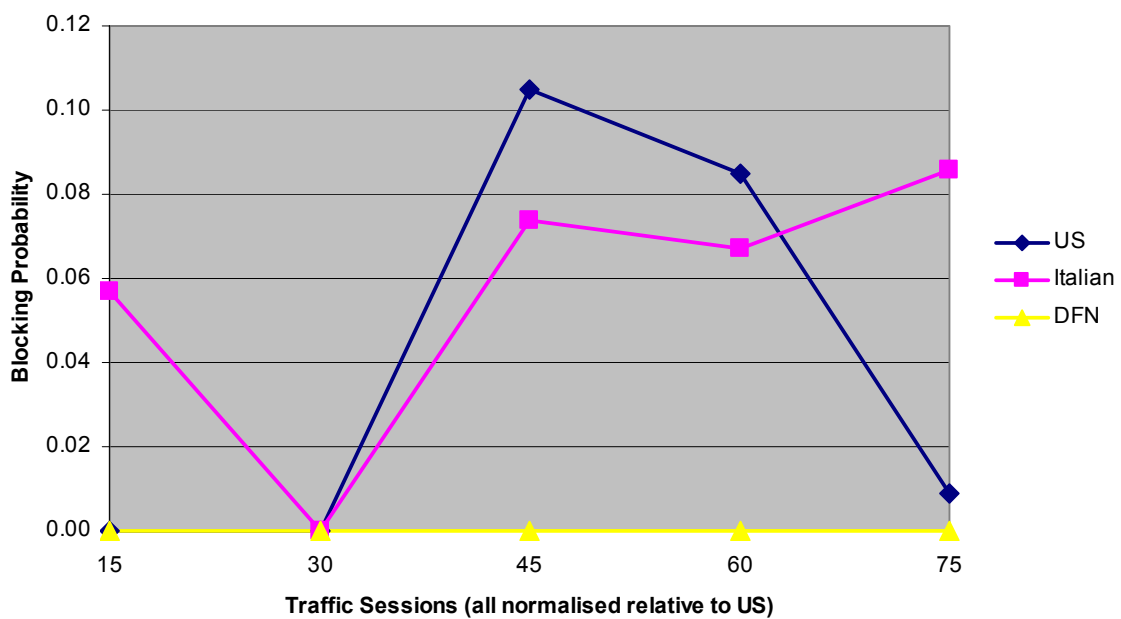
**Blocking Probability, 16 Wavelengths, High Number of Link Failures**

Figure 7.9: Blocking probability with 16 wavelengths and high number of link failures.

Table 7.10: Average overall blocking probability for all 360 simulation scenarios.

	Average overall blocking probability			
	2 Lambdas	4 Lambdas	8 Lambdas	16 Lambdas
<b>US</b>	0.160	0.025	0.028	0.029
<b>ITA</b>	0.093	0.026	0.027	0.012
<b>DFN</b>	0.014	0.009	0.013	0.003

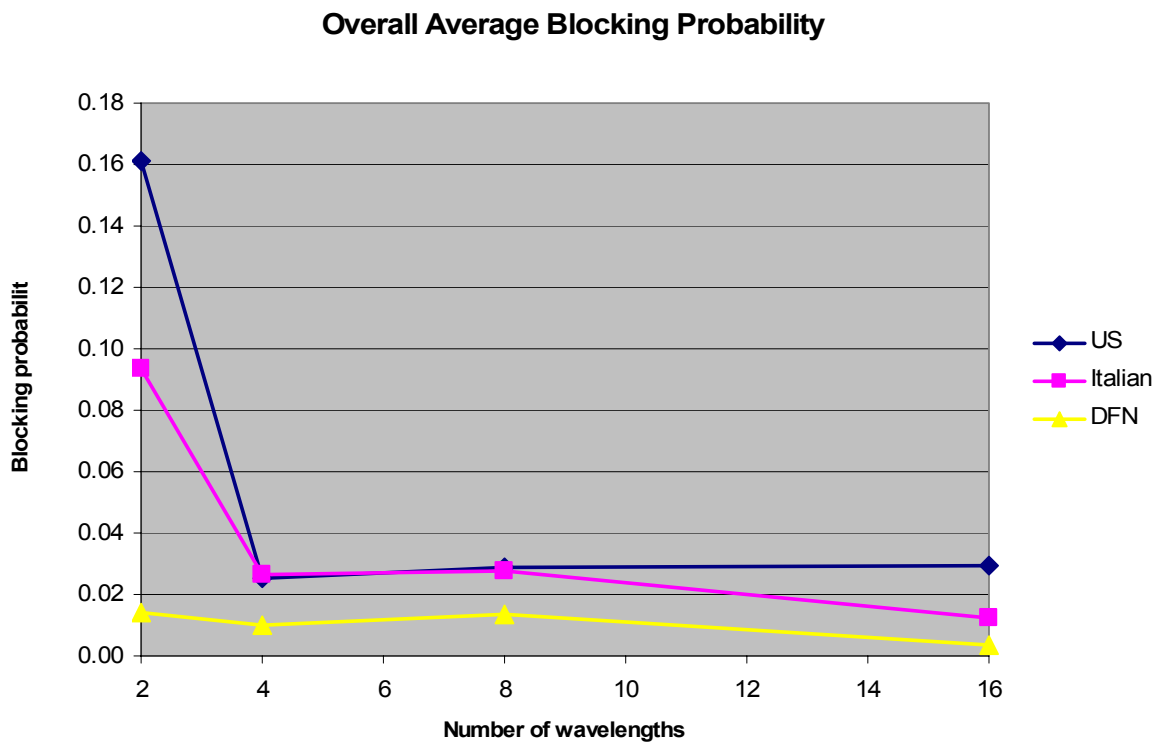


Figure 7.10: Average overall blocking probability for all 360 simulation scenarios.

The reason for the system's slightly higher (i.e. worse) blocking probability at 8 wavelengths versus 4 wavelengths, can be attributed to the low number of simulations, namely 5, per scenario. It is recommended that in future work, the number of simulations per scenario be increased by a factor of 10. This should ensure that a single simulation run with unusually low or high blocking probability will not have an undue influence.

## 7.2 Path usage

In figures 7.11 through 7.13, the results are shown for different path usage of the simulation scenarios, with increasing number of available wavelengths on the x axis. The results reflect a wide range of link failure and traffic load conditions presented in tables 6.3 and 6.4. The sum of the usage of path 1, path 2 and path 3 for a specific scenario is 100%.

In figure 7.11, the path usage of the first path in all topologies is shown. It can be seen that the usage (in percentage) of path 1 is the lowest in the topology with low connectivity (the US backbone network), and highest in the topology with the highest connectivity (the DFN network). If it is taken into account that, in the simulation setup, the first path is always used first if available, it means that, in topologies with low connectivities the first path will be used up before it will be used up in topologies with higher connectivities. This confirms the advantage that topologies of higher connectivities offer, namely that on average every node has access to more network resources, leading to lower blocking probabilities.

In figure 7.12, the path usage of the second path in all topologies is shown. It can be seen that as more wavelengths become available per link, the path usage for path 2 decreases. This is true for all topologies.

In figure 7.13, the path usage of the third path in all topologies is shown. The usage of path 3 is at a maximum (2.35%) in the US topology when only 2 wavelengths per link are available. This means that the implementation of a third path in this scenario leads to a sizeable reduction of the blocking probability. The usage of the third path significantly decreases in topologies with higher connectivities and increased wavelengths, thereby decreasing the advantage obtained by the inclusion of a third possible path.

Table 7.11: Usage of path 1 with increasing number of available wavelengths.

	Path usage, path 1 (%)			
	2 Lambdas	4 Lambdas	8 Lambdas	16 Lambdas
<b>US</b>	83.08	94.40	93.28	91.23
<b>Italian</b>	89.14	93.17	92.50	94.63
<b>DFN</b>	90.00	94.43	92.83	97.34

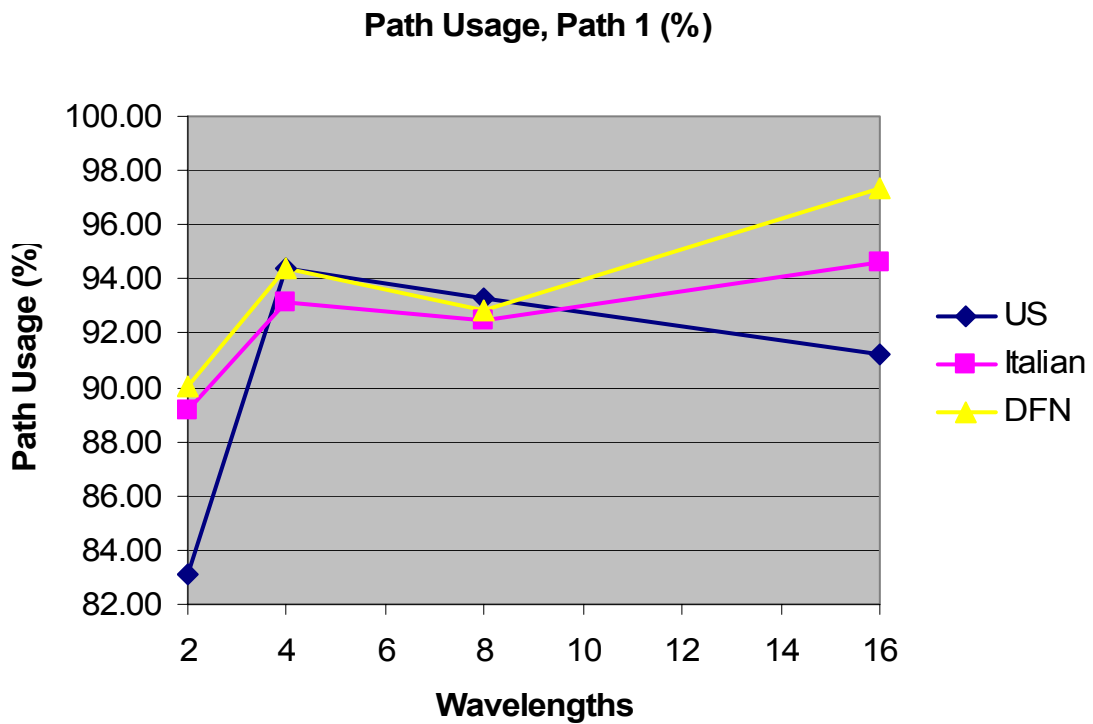


Figure 7.11: Usage of path 1 with increasing number of available wavelengths.

Table 7.12: Usage of path 2 with increasing number of available wavelengths.

	Path usage, path 2 (%)			
	2 Lambdas	4 Lambdas	8 Lambdas	16 Lambdas
<b>US</b>	14.57	5.23	5.65	7.82
<b>Italian</b>	10.37	6.61	7.26	4.91
<b>DFN</b>	8.85	4.22	6.50	2.58

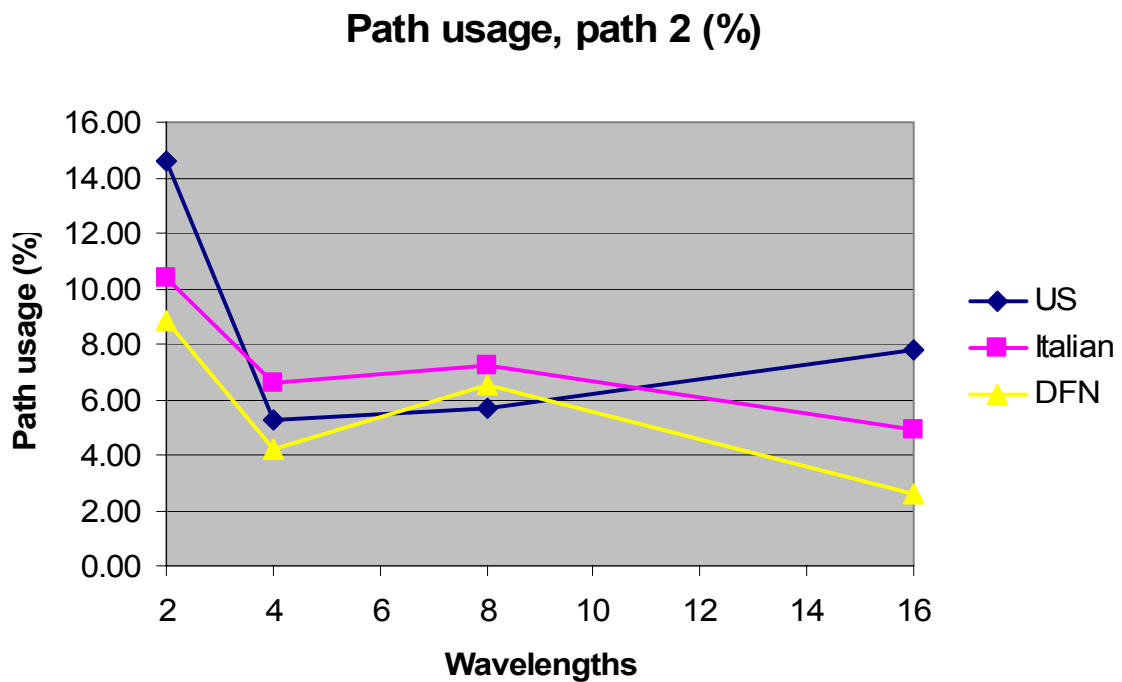


Figure 7.12: Usage of path 2 with increasing number of available wavelengths.



Table 7.13: Usage of path 3 with increasing number of available wavelengths.

	Path usage, path 3 (%)			
	2 Lambdas	4 Lambdas	8 Lambdas	16 Lambdas
<b>US</b>	2.35	0.37	1.07	0.94
<b>Italian</b>	0.49	0.22	0.24	0.46
<b>DFN</b>	1.14	1.35	0.67	0.07

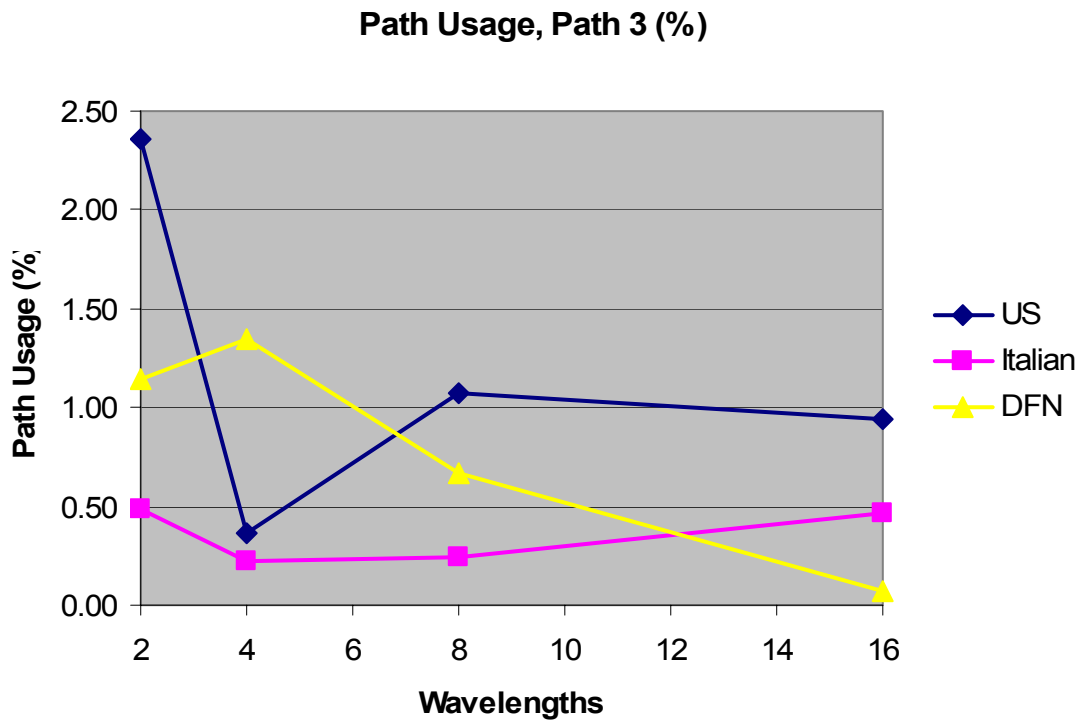


Figure 7.13: Usage of path 3 with increasing number of available wavelengths.

### 7.3 Link utilization

Table 7.14: Link utilization with increasing number of available wavelengths.

	Link utilization			
	2 Lambdas	4 Lambdas	8 Lambdas	16 Lambdas
<b>US</b>	0.201	0.125	0.120	0.130
<b>Italian</b>	0.160	0.139	0.110	0.087
<b>DFN</b>	0.114	0.073	0.074	0.045

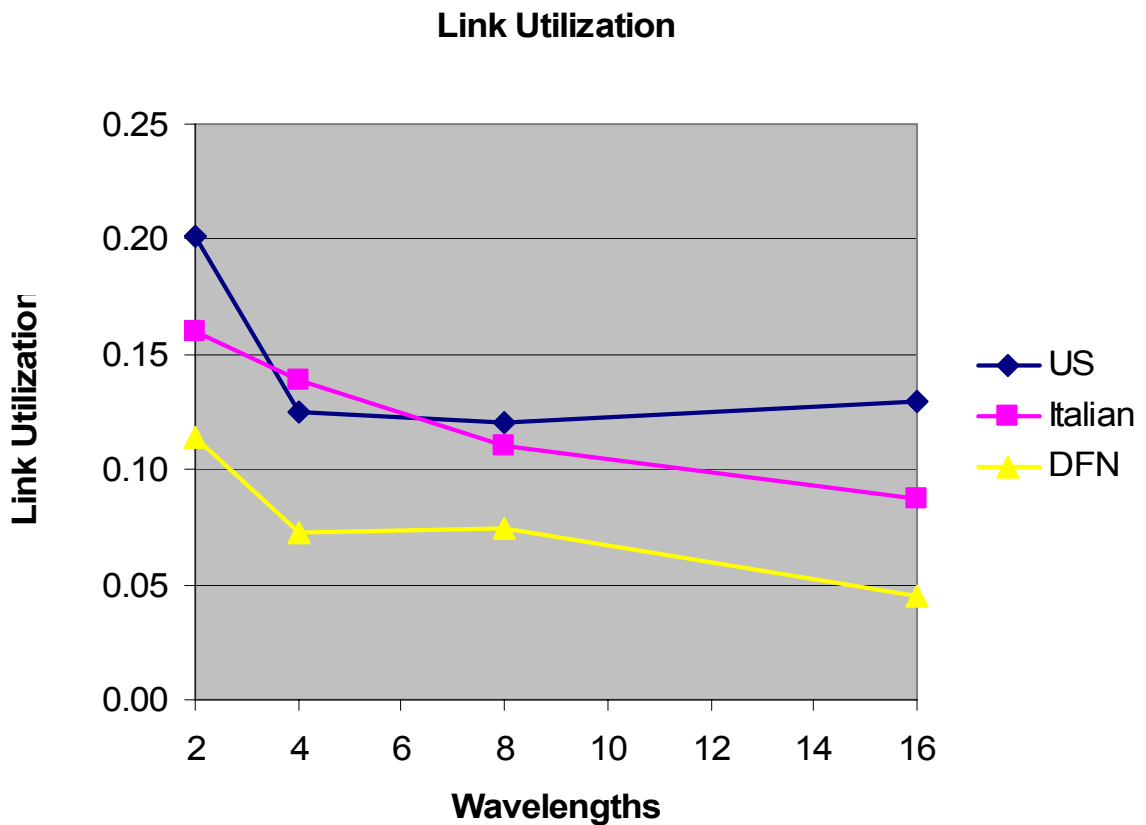


Figure 7.14: Link utilization with increasing number of available wavelengths.

# Chapter 8

## Conclusion

### 8.1 Summary

Fiber optic networks have become the technology of choice for transferring huge volumes of data traffic across large distances. Recently, fiber optics has also been making inroads with regard to intra-city communications. Within city limits, two of the most common causes of link failures are construction activity and vandalism. With this in mind, it is vital that the network designer has access to tools that enable him or her to simulate the effects that failures has on a network.

In this work, the author increased the scope and functionality of NS2 and OWns by adding protection functionality to the system. The routing and wavelength assignment algorithm was also further extended by the addition of a third possible path for all traffic flows. The network designer is now able to simulate the effect that single or multiple link failures will have on network performance with a tool that is open source.

The results of the simulations were found to be informative and a summary of the conclusions can be found below.

### 8.2 Assessment

*A network that has a lower degree of connectivity is at higher risk than a network with a higher degree of connectivity when link failures occur.* This intuitive observation is proved by the simulation results: the United States backbone network has the lowest degree of connectivity of the 3 topologies tested, and has the highest average blocking probability. The Italian backbone network, that has a degree of connectivity slightly higher than the

United States backbone network, has a blocking probability that is generally slightly lower than the United States backbone network. The DFN network, that has a degree of connectivity significantly higher than the other two topologies, has an average blocking probability that is significantly lower than the other two topologies. The inaccuracies brought about by the inability to totally normalise the parameters of the three systems with respect to each other is generally in the lower single digit percentage range, and can safely be ignored.

These results can be attributed to the fact that in networks with higher connectivity, a link failure has a lower impact due to the fact that traffic flows have a choice of more alternate disjoint paths, as well as the fact that the traffic is distributed over more links, leading to a lower traffic load per link.

*In networks with low connectivity, few available wavelengths lead to unacceptably high blocking probabilities when traffic volumes are high and / or many link failures occur.* The advantage offered by networks with higher connectivities is especially marked when limited wavelengths are available; as available wavelengths increase, the blocking probability advantage lessens.

These results suggest that networks with low degrees of connectivity and few wavelengths are especially at risk of poor performance when congestion occurs. These risks can be greatly reduced with the addition of more wavelengths; this upgrade to WDM or CWDM is more cost effective than the laying of new underground fiber optic cables. This cost-saving option is widely implemented in industry.

*The addition of a third path brings about a small, but measurable, improvement to network performance. This addition is especially discernable when applied to networks with low connectivity and limited wavelengths.* The maximum usage of path 3 occurred with the United States backbone network with 2 available wavelengths, namely a path 3 usage of 2.5%. This usage significantly lessened with more available wavelengths, and topologies with higher connectivities.

The advantage, though minimal, would be very cost effective to implement in industry. This is due to the fact that only an upgrade in software, and possibly processing power, would be required by the computers in charge of the routing operation. No capital expenditure would be required on any optical equipment in the network.

*The time required to reroute a traffic flow from an interrupted primary path to an available alternate path is well within the time required by industry.* The average measured time for the protection mechanism to be implemented was measured to be 90 milliseconds.

### **8.3 Future work**

A possible continuation of this work may entail the implementation of a restoration mechanism in NS2 and OWns. It will be extremely informative to see if the expected improvement in blocking probability and expected increase in restoration time of a restoration mechanism compared to a protection mechanism do indeed materialise.

It is also recommended that in future, the distance between nodes in a network is taken into consideration. This will lead to more accurate simulations, since longer links are more likely to fail than shorter links.

## References

- [1] J.M.H. Elmirghani, H.T. Mouftah, "Technologies and architectures for scalable dynamic dense WDM networks," *IEEE Communications Magazine*, Vol 38, no 2, pp. 58–66, February 2000.
- [2] P. Green, "Progress in Optical Networking," *IEEE Communications Magazine*, Vol 39, no 1, pp. 54-61, January 2001.
- [3] I. Chlamtac, A. Ganz, G. Karmi, "Lightpath communications: an approach to high bandwidth optical WAN's," *IEEE Transactions on Communications*, Vol 40, no 7, pp. 1171-1182, July 1992.
- [4] H.V. Madhyastha, N. Balakrishnan, "An efficient algorithm for virtual-wavelength-path routing minimizing average number of hops," *IEEE Journal on Selected Areas in Communications*, Vol 21, no 9, pp. 1433-1440, November 2003.
- [5] International Telecommunication Union, *Recommendation G.694.1 – Spectral grids for WDM applications: DWDM frequency grid*, June 2002.
- [6] International Telecommunication Union, *Recommendation G.694.2 – Spectral grids for WDM applications: CWDM wavelength grid*, December 2003.
- [7] D.R. Kuhn, "Sources of failure in the public switched telephone network," *IEEE Computer Magazine*, Vol 30, no 4, pp. 31-36, April 1997.
- [8] C. Ou, K. Zhu, H. Zang, L.H. Sahasrabudde, B. Mukherjee, "Traffic grooming for survivable WDM networks - shared protection," *IEEE Journal on Selected Areas in Communications*, Vol 21, no 9, pp. 1367-1383, November 2003.

- [9] G. Keiser, *Optical fiber communications*. McGraw-Hill, 2000.
- [10] “Optilan fiber product range,” [http://www.optilan.com/Prodrange/Cable Range/Microsoft Word - FTN-cable\\_1\\_.pdf](http://www.optilan.com/Prodrange/CableRange/Microsoft Word - FTN-cable_1_.pdf), last visited: 19 February 2005.
- [11] “Redfern Broadband Networks Inc. Characteristics of CWDM. Roots, current status & future opportunities,” [http://www.rbni.com/rbn\\_cwdm\\_tech\\_paper-1\\_20sep02.pdf](http://www.rbni.com/rbn_cwdm_tech_paper-1_20sep02.pdf), last visited: 19 February 2005.
- [12] S.O. Kasap, *Optoelectronics*. Prentice-Hall, 1999.
- [13] K. Konno, O. Matsushima, D. Navarro, K. Hara, G. Suzuki, M. Miura-Mattausch, “Towards current-characteristic simulation of p-i-n photodiodes based on spectral method”, [http://www.rcis.hiroshima-u.ac.jp/21coe/pdf/2nd\\_WS/Poster.13-P.130.pdf](http://www.rcis.hiroshima-u.ac.jp/21coe/pdf/2nd_WS/Poster.13-P.130.pdf), last visited: 20 September 2005.
- [14] “New C-band EDFA,” <http://www.tycoelectronics.com/fiberoptics/146.pdf>, last visited: 16 January 2005.
- [15] “Alcatel repeatered submarine systems,” <http://www.alcatel.com/submarine/products/repeater/index.html>, last visited: 19 February 2005.
- [16] R. Chen, G.F Fernando, T. Butler, R.A. Badcock, “A novel ultrasound fiber optic sensor based on a fused-tapered optical fibre coupler,” *Institute of Physics Publishing: Measurement Science and Technology*, pp. 1490-1495, July 2004.
- [17] P.S. André, J.L. Pinto, I. Abe, H.J. Kalinowski, O. Frazão, F.M. Araújo, “Fibre Bragg grating for telecommunications applications: tunable thermally stress enhanced OADM,” *Journal of Microwaves and Optoelectronics*, Vol 2, no 3, pp. 32-45, July 2001.

- [18] V.A. Aksyuk, S. Arney, N.R. Basavanhally, D.J. Bishop, C.A. Bolle, C.C. Chang, R. Frahm, A. Gasparyan, J.V. Gates, R. George, C.R. Giles, J. Kim, P.R. Kolodner, T.M. Lee, D.T. Neilson, C. Nijander, C.J. Nuzman, M. Paczkowski, A.R. Papazian, R. Ryf, H. Shea, M.E. Simon, "238x238 Surface micromachined optical crossconnect with 2dB maximum loss," *Optical Fiber Communications Conference 2002*, Anaheim, pp. 1-4, March 2002.
- [19] T. Chikama, H. Onaka, S. Kuroyanagi, "Photonic networking using optical add drop multiplexers and optical cross-connects," *Fujitsu Science Technology Journal*, pp. 46-55, July 1999.
- [20] "3D MEMS for optical cross-connect switches: a new means of managing network traffic,"  
[http://www.ptbmagazine.com/articles/Articles\\_on\\_File/May\\_2002/May\\_2002\\_article.html](http://www.ptbmagazine.com/articles/Articles_on_File/May_2002/May_2002_article.html), last visited: 19 February 2005.
- [21] American National Standards Institute, *ANSI Standard T1.105.06 – synchronous optical network (SONET) physical layer specifications*, 1996, amended August 2002.
- [22] International Telecommunication Union, *Recommendation G.957 – Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*, June 1999, amended 1 December 2003.
- [23] "Word alignment and SONET/SDH deframing,"  
<http://direct.xilinx.com/bvdocs/appnotes/xapp652.pdf>, last visited: 19 February 2005.
- [24] T. Russell, *Telecommunications pocket reference*. McGraw-Hill, 2000.
- [25] "Multiprotocol label switching (MPLS) traffic engineering,"



[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mppls\\_te.pdf](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mppls_te.pdf), last visited: 19 February 2005.

- [26] S. Okamoto, E. Oki, K. Shimano, A. Sahara, N. Yamanaka, "Demonstration of the highly reliable HIKARI router network based on a newly developed disjoint path selection scheme," *IEEE Communications Magazine*, Vol 40, no 11, pp. 52-59, November 2002.
- [27] S. Dixit, Y. Ye, "Streamlining the internet-fiber connection," *IEEE Spectrum*, Vol 38, no 4, pp. 52-57, April 2001.
- [28] Y. Lee, B. Mukherjee, "Traffic engineering in next-generation optical networks," pp. 1-50, April 2004.
- [29] C. Casetti, R.L. Cigno, M. Mellia, M. Munafo, "A new class of QoS routing strategies based on network graph reduction," *IEEE Infocom 2002*, New York, pp. 715-722, June 2002.
- [30] B.T. Doshi, R. Nagarajan, G.N.S. Prasanna, M.A. Qureshi, "Future WAN architecture driven by services, traffic volume, and technology trends," *Bell Labs Technical Journal*, pp. 13-32, January-June 2001.
- [31] D. Griffith, S. Lee, "A 1+1 protection architecture for optical burst switched networks," *IEEE Journal on Selected Areas in Communications*, Vol 21, no 9, pp. 1384-1398, November 2003.
- [32] R.R. Iraschko, W.D. Grover, "A highly efficient path-restoration protocol for management of optical network transport integrity," *IEEE Journal on Selected Areas in Communications*, Vol 18, no 5, pp. 779-794, May 2000.

- [33] A. Narula-Tam, P.J. Lin, E. Modiano, "Efficient routing and wavelength assignment for reconfigurable WDM networks," *IEEE Journal on Selected Areas in Communications*, Vol 20, no 1, pp. 75-88, January 2002.
- [34] Anonymous, *SDH: A pocket guide*. Wandel & Goltermann, volume 1.
- [35] B.E. Smith, "SONET self-healing networks," *Global Telecommunications Conference 1990*, San Diego, pp. 177-181, 1990.
- [36] A. Walsh, "Network and services integration forum (NSIF) reference architectures," pp. 1-44, October 2000.
- [37] "Switching and multiplexing,"  
<http://www.ece.northwestern.edu/~rberry/ECE333/Lect2001/lec19.pdf>, last visited: 20 February 2005.
- [38] W.D. Grover, J. Doucette, "Design of a meta-mesh of chain subnetworks: enhancing the attractiveness of mesh-restorable WDM networking on low connectivity graphs," *IEEE Journal on Selected Areas in Communications*, Vol 20, no 1, pp. 47-61, January 2002.
- [39] "DFN english home page," <http://www.dfn.de/content/en/enhome/index.html>, last visited: 18 February 2005.
- [40] "Aufbau des Gigabit-Wissenschaftsnetzes (G-WiN)," <http://www.dfn.de/DFN-Aufbau-GWiN1.pdf>, last visited: 18 February 2005.
- [41] P. Janse van Rensburg, Telkom, *personal e-mail correspondence*, 16 January 2005.
- [42] "SAT3 / WASC / SAFE topology," <http://www.safe-sat3.co.za/Configuration/Configuration.asp>, last visited: 18 February 2005.

- [43] “NEON communications corporate overview,”  
<http://www.neoninc.com/documents/146.pdf>, last visited: 18 February 2005.
- [44] W. Stallings, *Wireless communications and networks*. Prentice-Hall, 2002.
- [45] L. Roland, “High speed synchronous digital multiplexing systems,”  
[http://home.pages.at/tele/technik\\_tips/html\\_seiten/Sonet-sdh.htm](http://home.pages.at/tele/technik_tips/html_seiten/Sonet-sdh.htm), last accessed: 22 February 2005.
- [46] T. Russell, *Signalling System #7*, 3<sup>rd</sup> edition, McGraw-Hill, 2000.
- [47] X. Fang, R. Iraschko, R. Sharma, “All-optical four-fiber bidirectional line-switched ring,” *Journal of Lightwave Technology*, Vol 17, no 8, pp. 1302-1308, August 1999.
- [48] “Dijkstra’s algorithm,” [http://en.wikipedia.org/wiki/Dijkstra's\\_algorithm](http://en.wikipedia.org/wiki/Dijkstra's_algorithm), last accessed: 22 February 2005.
- [49] K. Fall, K. Varadhan, “The NS manual,”  
[http://www.isi.edu/nsnam/ns/doc/ns\\_doc.pdf](http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf), last visited: 20 February 2005.
- [50] E. Karasan, E. Ayanoglu, “Performance of WDM transport networks,” *IEEE Journal on Selected Areas in Communications*, Vol 16, no 7, pp. 1081-1096, September 1998.
- [51] E. Karasan, E. Ayanoglu, “Effects of wavelength routing and selection algorithms on wavelength conversion gain in WDM optical networks,” *IEEE/ACM Transactions on Networking*, Vol 6, no 2, pp. 186-196, April 1998.

- [52] K. Kar, M. Kodialam, T.V. Lakhsman, "Routing restorable bandwidth guaranteed connections using maximum 2-route flows," *IEEE/ACM Transactions on Networking*, Vol 11, no 5, pp. 772-781, October 2003.
- [53] Y. Miyao, H. Saito, "Optimal design and evaluation of survivable WDM transport networks," *IEEE Journal on Selected Areas in Communications*, Vol 16, no 7, pp. 1190-1198, September 1998.
- [54] S. Ramamurthy, L. Sahasrabudde, B. Mukherjee, "Survivable WDM mesh networks," *Journal on Lightwave Technology*, Vol 21, no 4, pp. 870-883, April 2003.
- [55] R.R. Iraschko, M.H. MacGregor, W.D. Grover, "Optimal capacity placement for path restoration in STM or ATM mesh-survivable networks," *IEEE/ACM Transactions on Networking*, Vol 6, no 3, pp. 325-336, June 1998.
- [56] D. Stamatelakis, W.D. Grover, "IP layer restoration and network planning based on virtual protection cycles," *IEEE Journal on Selected Areas on Communications*, Vol 18, no 10, pp. 1938-1949, October 2000.
- [57] W.D. Grover, "The self-healing network," *Proceedings of the IEEE Globecom 1987*, Tokyo, pp. 1090-1095, December 1987.
- [58] P.A. Veitch, R.S.K. Chng, D. Johnson, I. Hawker, D.G. Smith, "An integrated restoration system for SDH-based ATM transport networks," *IEEE Globecom 1996*, London, pp. 1882-1886, November 1996.
- [59] S. Ramamurthy, B. Mukherjee, "Survivable WDM networks, part II – restoration," *IEEE ICC 1999*, Vancouver, pp. 2023-2030, June 1999.
- [60] "NEST home page," <ftp://ftp.cs.columbia.edu/nest>, last visited: 18 February 2005.

- [61] "REAL home page," <http://www.cs.cornell.edu/skeshav/real/>, last visited: 18 February 2005.
- [62] "BONeS home page," <http://www.cadence.com>, last visited: 18 February 2005.
- [63] "OPNET home page," <http://www.opnet.com>, last visited: 18 February 2005.
- [64] "OPNET WDM guru brochure,"  
<http://www.opnet.com/products/wdmguru/wdmguru.pdf>, last visited: 18 February 2005.
- [65] "NS1 home page," <http://www.isi.edu/nsnam/ns/index.html>, last visited: 18 February 2005.
- [66] "VINT home page," <http://netweb.usc.edu/vint>, last visited: 18 February 2005.
- [67] "NS2 download page," <http://www.isi.edu/nsnam/ns/ns-build.html>, last visited: 18 February 2005.
- [68] H. Brits, "Development of a GUI for NS2," *University of Pretoria, Department of Electrical, Electronic and Computer Engineering*, final year project, 2004.
- [69] M. Greiss, "Tutorial for the network simulator NS,"  
<http://www.isi.edu/nsnam/ns/tutorial/nsindex.html>, last visited: 20 February 2005.
- [70] "OWns source code package," <http://www.eecs.wsu.edu/~dawn/software/owns-src.tar.gz>, last visited: 22 February 2005.
- [71] B. Wen, M. Bhide, R.K. Shenai, K.M. Sivalingam, "Optical wavelength division multiplexing (WDM) network simulator (OWns): architecture and performance studies," *SPIE Optical Networks Magazine*, pp. 1-22, March 2001.

- [72] M.J. O'Mahony, D. Simeonidou, D.K. Hunter, A. Tzanakaki, "The application of optical packet switching in future communication networks," *IEEE Communications Magazine*, Vol 39, no 3, pp. 128-135, March 2001.
- [73] G. Conte, M. Listani, M. Settembre, R. Sabella, "Strategy for protection and restoration of optical paths in WDM backbone networks for next-generation internet infrastructures," *Journal of Lightwave Technology*, Vol 20, no 8, pp. 1264-1276, August 2002.
- [74] R. Geldenhuys, F.W. Leuschner, Y. Liu, G.D. Khoe, N. Calabretta, H.J.S. Dorren, "Selecting fiber delay line distributions for traveling buffers in an all-optical packet switched cross-connect," *CCECE 2003*, pp. 1-4, Montreal, May 2003.
- [75] C. Lo, B. Chuang, "A novel approach of backup path reservation for survivable high-speed networks," *IEEE Communications Magazine*, Vol 41, no 3, pp. 146-152, March 2003.

# Appendix A

## Complete simulation results

Table A.1: Complete results – United States backbone network

United States 28 node network									
$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
2	0	15	0	4.333333	0.26143	0.111111	95.24	4.76	0.00
2	0	30	0.027027	3.777777	0.220979	0.125253	83.33	13.89	2.78
2	0	45	0.181818	3.708333	0.187644	0.169293	80.56	16.67	2.78
2	0	60	0.108433	3.391891	0.158626	0.157576	83.78	14.86	1.35
2	0	75	0.230088	3.505747	0.158684	0.255556	82.95	14.77	2.27
2	2	15	0	4.333333	0.261436	0.111111	95.24	4.76	0.00
2	2	30	0.027027	3.777777	0.220495	0.125253	83.33	13.89	2.78
2	2	45	0.197802	3.767123	0.181622	0.178586	80.82	16.44	2.74
2	2	60	0.108433	3.391891	0.158626	0.157576	83.78	14.86	1.35
2	2	75	0.3	3.511904	0.155466	0.284444	77.38	21.43	1.19
2	4	15	0	4.333333	0.261436	0.111111	95.24	4.76	0.00
2	4	30	0.027027	3.777777	0.220979	0.125253	83.33	13.89	2.78
2	4	45	0.193548	3.773333	0.190246	0.173737	81.33	16.00	2.67
2	4	60	0.108433	3.391891	0.158626	0.157576	83.78	14.86	1.35
2	4	75	0.325203	3.578313	0.152746	0.348889	75.90	19.28	4.82
2	6	15	0.043478	4.318181	0.270462	0.134343	86.36	13.64	0.00
2	6	30	0.1	3.861111	0.213688	0.189899	80.56	16.67	2.78
2	6	45	0.2	3.694444	0.176986	0.214545	84.51	12.68	2.82
2	6	60	0.191011	3.430555	0.159649	0.253535	76.39	22.22	1.39
2	6	75	0.272727	3.693181	0.171715	0.32	72.73	22.73	4.55
2	8	15	0.178571	5	0.187779	0.228283	82.61	13.04	4.35
2	8	30	0.166666	3.8	0.227071	0.169697	85.71	11.43	2.86
2	8	45	0.2	3.694444	0.188046	0.217374	86.30	10.96	2.74
2	8	60	0.163043	3.454545	0.157128	0.224242	79.22	19.48	1.30
2	8	75	0.314049	3.566265	0.160146	0.342222	77.11	16.87	6.02
2	10	15	0.193548	4.52	0.240812	0.226263	84.00	16.00	0.00
2	10	30	0.216923	3.861111	0.219554	0.189899	80.56	16.67	2.78
2	10	45	0.25	3.813333	0.182863	0.237374	86.30	10.96	2.74
2	10	60	0.229775	3.273972	0.152976	0.171717	86.30	10.96	2.74
2	10	75	0.273504	3.682352	0.156197	0.323333	77.65	17.65	4.71
4	0	15	0	4.238095	0.249803	0.052525	100.00	0.00	0.00

$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
4	0	30	0	3.459459	0.211722	0.058081	100.00	0.00	0.00
4	0	45	0	3.302631	0.173193	0.109596	98.68	1.32	0.00
4	0	60	0	3.346153	0.160256	0.079979	98.72	1.28	0.00
4	0	75	0.01	3.414141	0.158751	0.158751	95.96	3.03	1.01
4	2	15	0	4.238095	0.249803	0.052525	100.00	0.00	0.00
4	2	30	0	3.459459	0.211722	0.058081	100.00	0.00	0.00
4	2	45	0.012345	3.7125	0.173938	0.138384	96.30	3.70	0.00
4	2	60	0	3.346153	0.159656	0.079798	98.72	1.28	0.00
4	2	75	0.01	3.414141	0.158751	0.141358	95.96	3.03	1.01
4	4	15	0.038461	4.68	0.237154	0.094949	96.00	4.00	0.00
4	4	30	0.066666	3.5	0.21243	0.110101	90.48	9.52	0.00
4	4	45	0	3.302631	0.173193	0.109596	97.37	2.63	0.00
4	4	60	0	3.346153	0.163513	0.079798	96.15	2.56	1.28
4	4	75	0.0099	3.44	0.156701	0.148765	96.00	3.00	1.00
4	6	15	0	4.238095	0.249568	0.052525	100.00	0.00	0.00
4	6	30	0.01	3.459459	0.211722	0.058081	100.00	0.00	0.00
4	6	45	0.012345	3.4625	0.172345	0.10697	96.25	3.75	0.00
4	6	60	0	3.346153	0.160256	0.079798	98.72	1.28	0.00
4	6	75	0.057142	3.50505	0.154488	0.199306	87.88	11.11	1.01
4	8	15	0.038461	4.68	0.24059	0.094949	92.00	8.00	0.00
4	8	30	0.045454	3.809523	0.224628	0.182323	90.48	9.52	0.00
4	8	45	0.122222	3.848101	0.183115	0.201667	88.61	8.86	2.53
4	8	60	0.0125	3.346153	0.161086	0.079798	90.91	9.09	0.00
4	8	75	0.057692	3.55102	0.15669	0.248611	87.76	11.22	1.02
4	10	15	0.023529	4.92	0.261222	0.161616	88.00	12.00	0.00
4	10	30	0.045454	3.880952	0.214335	0.220202	85.71	14.29	0.00
4	10	45	0.057142	3.493975	0.184812	0.227778	89.16	10.84	0.00
4	10	60	0.107142	3.417721	0.156625	0.185859	88.24	11.76	0.00
4	10	75	0.02	3.530612	0.156644	0.190972	87.91	9.89	2.20
8	10	15	0	4.238095	0.258029	0.044444	100.00	0.00	0.00
8	0	30	0	3.459459	0.218877	0.036616	100.00	0.00	0.00
8	0	45	0	3.289473	0.178052	0.084343	100.00	0.00	0.00
8	0	60	0	3.307692	0.165173	0.057828	100.00	0.00	0.00
8	0	75	0	3.363636	0.16302	0.099383	100.00	0.00	0.00
8	2	15	0	4.238095	0.258029	0.044444	100.00	0.00	0.00
8	2	30	0.022222	3.795454	0.224312	0.110455	91.30	6.52	2.17
8	2	45	0	3.324675	0.173184	0.090404	100.00	0.00	0.00
8	2	60	0	3.307692	0.165173	0.057828	100.00	0.00	0.00
8	2	75	0	3.363636	0.162496	0.09383	100.00	0.00	0.00
8	4	15	0.055555	3.617647	0.264014	0.135353	94.12	5.88	0.00
8	4	30	0.076923	3.625	0.220681	0.146212	91.84	8.16	0.00
8	4	45	0	3.289473	0.178052	0.084343	95.00	5.00	0.00
8	4	60	0	3.307692	0.165173	0.057828	94.38	5.62	0.00
8	4	75	0	3.64423	0.16434	0.197222	87.50	11.54	0.96
8	6	15	0.068965	5.259259	0.261394	0.183586	88.89	7.41	3.70
8	6	30	0.04	4.104166	0.224254	0.207828	91.67	6.25	2.08
8	6	45	0.048192	3.35443	0.175277	0.117222	93.75	6.25	0.00
8	6	60	0.097826	3.626506	0.1594	0.22702	85.54	14.46	0.00



$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
8	6	75	0	3.363636	0.163045	0.199383	84.85	13.13	2.02
8	8	15	0	4.318181	0.257988	0.062626	100.00	0.00	0.00
8	8	30	0	3.459459	0.218877	0.036616	100.00	0.00	0.00
8	8	45	0.047619	3.4625	0.182908	0.165657	92.50	5.00	2.50
8	8	60	0.011235	3.53409	0.161269	0.116919	88.64	9.09	2.27
8	8	75	0.074766	3.525252	0.162021	0.173264	90.91	8.08	1.01
8	10	15	0.066666	4.392857	0.234338	0.10202	92.86	7.14	0.00
8	10	30	0.043478	3.886363	0.233555	0.161869	85.71	9.52	4.76
8	10	45	0.03409	3.388235	0.178863	0.182071	84.71	14.12	1.18
8	10	60	0.163265	4.219512	0.168335	0.233939	81.71	13.41	4.88
8	10	75	0.009009	3.363636	0.161669	0.110802	82.41	12.96	4.63
16	0	15	0	4.238095	0.274632	0.038889	100.00	0.00	0.00
16	0	30	0	3.459459	0.23311	0.03347	100.00	0.00	0.00
16	0	45	0	3.289473	0.188921	0.074621	100.00	0.00	0.00
16	0	60	0	3.307692	0.174705	0.043662	100.00	0.00	0.00
16	0	75	0	3.363636	0.172372	0.091358	100.00	0.00	0.00
16	2	15	0	4.238095	0.275244	0.038888	100.00	0.00	0.00
16	2	30	0.023829	3.590909	0.256946	0.138485	91.30	6.52	2.17
16	2	45	0	3.324675	0.188152	0.070682	100.00	0.00	0.00
16	2	60	0	3.307692	0.174705	0.083662	94.87	5.13	0.00
16	2	75	0.071428	3.682692	0.172189	0.210139	82.69	17.31	0.00
16	4	15	0	4.238095	0.274632	0.038888	100.00	0.00	0.00
16	4	30	0	3.459459	0.233104	0.03447	100.00	0.00	0.00
16	4	45	0.074757	3.729411	0.176932	0.200154	91.67	5.95	2.38
16	4	60	0.017526	3.626506	0.170243	0.193308	85.54	14.46	0.00
16	4	75	0.074468	3.413793	0.178759	0.181435	81.61	12.64	5.75
16	6	15	0	4.238095	0.274632	0.038889	100.00	0.00	0.00
16	6	30	0	4.066666	0.243125	0.144798	88.89	11.11	0.00
16	6	45	0	3.290697	0.179609	0.178056	89.53	10.47	0.00
16	6	60	0.043478	3.681818	0.187728	0.167361	79.55	20.45	0.00
16	6	75	0.023255	3.904761	0.169617	0.300556	82.14	16.67	1.19
16	8	15	0	4.68	0.236199	0.081313	92.00	8.00	0.00
16	8	30	0.105263	3.77551	0.263969	0.150909	86.00	8.00	6.00
16	8	45	0.071428	3.65934	0.19361	0.250586	80.22	18.68	1.10
16	8	60	0.08421	3.666666	0.174094	0.214167	80.46	19.54	0.00
16	8	75	0.092448	3.511627	0.19528	0.232222	81.40	17.44	1.16
16	10	15	0	4.238095	0.274768	0.038888	100.00	0.00	0.00
16	10	30	0	3.545454	0.235155	0.078788	93.18	6.82	0.00
16	10	45	0.105263	3.682352	0.180856	0.220556	87.06	10.59	2.35
16	10	60	0.085185	3.681818	0.177623	0.208333	82.95	13.64	3.41
16	10	75	0.009345	3.735849	0.169204	0.13125	85.85	11.32	2.83

Table A.2: Complete results – Italian backbone network

Italian 21 node network									
$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
2	0	12	0	3.2	0.13674	0.056818	100.00	0.00	0.00
2	0	23	0.04	2.541666	0.093323	0.044192	95.83	4.17	0.00
2	0	35	0.021276	2.913043	0.127082	0.09596	97.83	2.17	0.00
2	0	46	0.14754	3.173076	0.165992	0.19697	86.54	11.54	1.92
2	0	58	0.164705	2.887323	0.151444	0.283333	77.46	22.54	0.00
2	2	12	0.055555	3	0.139522	0.079545	94.12	5.88	0.00
2	2	23	0.04	2.541666	0.093323	0.044192	95.83	4.17	0.00
2	2	35	0.021276	2.913043	0.127955	0.09596	97.83	2.17	0.00
2	2	46	0.14754	3.173076	0.165992	0.19697	86.54	11.54	1.92
2	2	58	0.164705	2.887323	0.150084	0.283333	77.46	22.54	0.00
2	3	12	0	3.2	0.13647	0.056818	100.00	0.00	0.00
2	3	23	0.04	2.541666	0.093323	0.044192	95.83	4.17	0.00
2	3	35	0.021276	2.913043	0.127007	0.09596	97.83	2.17	0.00
2	3	46	0.14754	3.173076	0.166113	0.19697	86.54	11.54	1.92
2	3	58	0.22093	2.925373	0.15752	0.334596	76.12	20.90	2.99
2	5	12	0	3.2	0.13647	0.056818	100.00	0.00	0.00
2	5	23	0.04	2.541666	0.093323	0.04419	95.83	4.17	0.00
2	5	35	0.115384	3.021739	0.127513	0.20508	82.61	17.39	0.00
2	5	46	0.220588	3.226415	0.151962	0.348485	81.13	16.98	1.89
2	5	58	0.168674	2.927536	0.151168	0.313889	76.81	23.19	0.00
2	6	12	0	3.2	0.13647	0.056818	100.00	0.00	0.00
2	6	23	0.04	2.541666	0.093332	0.044192	95.83	4.17	0.00
2	6	35	0.041666	2.913043	0.127082	0.09596	97.83	2.17	0.00
2	6	46	0.14754	3.173076	0.168111	0.19697	86.54	11.54	1.92
2	6	58	0.191011	2.930555	0.149769	0.327778	76.39	23.61	0.00
2	8	12	0.052631	3.444444	0.138582	0.125	83.33	16.67	0.00
2	8	23	0.038461	2.52	0.117128	0.058081	92.00	8.00	0.00
2	8	35	0.057692	3.081632	0.146004	0.199495	87.76	12.24	0.00
2	8	46	0.193548	3.22	0.165789	0.236111	82.00	16.00	2.00
2	8	58	0.260416	2.929577	0.154412	0.397222	70.42	29.58	0.00
4	0	12	0	3.2	0.138567	0.028409	100.00	0.00	0.00
4	0	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	0	35	0	2.869565	0.129177	0.050505	100.00	0.00	0.00
4	0	46	0	3	0.153062	0.092172	100.00	0.00	0.00
4	0	58	0.014084	2.828571	0.14841	0.154321	95.00	5.00	0.00
4	2	12	0.086956	4.047619	0.13436	0.225379	76.19	23.81	0.00
4	2	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	2	35	0	2.869565	0.129177	0.050505	100.00	0.00	0.00
4	2	46	0	3.25862	0.156782	0.189394	94.83	5.17	0.00
4	2	58	0.014084	2.828571	0.147937	0.154321	95.71	4.29	0.00
4	3	12	0	3.2	0.138567	0.028409	100.00	0.00	0.00
4	3	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	3	35	0	2.869565	0.129177	0.050505	100.00	0.00	0.00
4	3	46	0.034482	3.357142	0.150361	0.210859	87.50	12.50	0.00

$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
4	3	58	0.081265	2.704225	0.14701	0.203704	90.14	9.86	0.00
4	5	12	0	3.2	0.138446	0.028409	100.00	0.00	0.00
4	5	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	5	35	0	2.87755	0.129829	0.101641	100.00	0.00	0.00
4	5	46	0	3	0.153062	0.092172	100.00	0.00	0.00
4	5	58	0.061728	3	0.148049	0.3125	86.84	13.16	0.00
4	6	12	0.086956	3.904761	0.137737	0.257576	77.78	22.22	0.00
4	6	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	6	35	0.067796	3.254545	0.135054	0.346591	85.45	10.91	3.64
4	6	46	0.032258	3.4	0.155953	0.291035	86.67	11.67	1.67
4	6	58	0.101951	3.097222	0.140428	0.310185	79.17	20.83	0.00
4	8	12	0.074074	3.904761	0.137737	0.257576	80.95	19.05	0.00
4	8	23	0	2.64	0.094835	0.022096	100.00	0.00	0.00
4	8	35	0	2.869565	0.129177	0.050505	100.00	0.00	0.00
4	8	46	0.064516	3.534482	0.151089	0.306818	82.76	17.24	0.00
4	8	58	0.074074	2.84	0.154694	0.269097	76.00	22.67	1.33
8	0	12	0	3.2	0.142876	0.019886	100.00	0.00	0.00
8	0	23	0	2.64	0.097822	0.013889	100.00	0.00	0.00
8	0	35	0	2.869565	0.133316	0.037879	100.00	0.00	0.00
8	0	46	0	3	0.158042	0.061869	100.00	0.00	0.00
8	0	58	0	2.771428	0.148829	0.104167	100.00	0.00	0.00
8	2	12	0	3.2	0.142876	0.019886	100.00	0.00	0.00
8	2	23	0	2.64	0.097822	0.013888	100.00	0.00	0.00
8	2	35	0.018867	3.038461	0.141865	0.178662	86.54	13.46	0.00
8	2	46	0	3	0.157911	0.061869	100.00	0.00	0.00
8	2	58	0	2.771428	0.148829	0.104167	100.00	0.00	0.00
8	3	12	0	3.2	0.142876	0.019886	100.00	0.00	0.00
8	3	23	0	2.576923	0.097956	0.016414	100.00	0.00	0.00
8	3	35	0.145161	3.509433	0.144654	0.269571	71.70	26.42	1.89
8	3	46	0	2.982142	0.158341	0.068182	100.00	0.00	0.00
8	3	58	0	2.780821	0.148831	0.127315	100.00	0.00	0.00
8	5	12	0	3.2	0.142876	0.019886	100.00	0.00	0.00
8	5	23	0	2.64	0.097822	0.013889	100.00	0.00	0.00
8	5	35	0.056603	3.34	0.129854	0.156566	92.00	8.00	0.00
8	5	46	0.013333	2.76923	0.151037	0.164187	81.54	18.46	0.00
8	5	58	0.051948	3.356164	0.138803	0.233507	80.82	19.18	0.00
8	6	12	0	3	0.144276	0.035038	100.00	0.00	0.00
8	6	23	0	2.64	0.097822	0.013889	100.00	0.00	0.00
8	6	35	0	2.869565	0.133316	0.037879	100.00	0.00	0.00
8	6	46	0.094594	3.059701	0.147672	0.258929	73.13	25.37	1.49
8	6	58	0	2.816901	0.147222	0.127315	100.00	0.00	0.00
8	8	12	0.2	4.1875	0.174179	0.337121	56.25	43.75	0.00
8	8	23	0	2.64	0.097822	0.013889	100.00	0.00	0.00
8	8	35	0.055555	3.45098	0.13419	0.231061	76.47	19.61	3.92
8	8	46	0.102564	2.657142	0.139168	0.270833	74.29	25.71	0.00
8	8	58	0.0875	3.260273	0.139886	0.279514	82.19	17.81	0.00
16	0	12	0	3.2	0.151438	0.019255	100.00	0.00	0.00

$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
16	0	23	0	2.64	0.103864	0.013258	100.00	0.00	0.00
16	0	35	0	2.869565	0.141917	0.03267	100.00	0.00	0.00
16	0	46	0	3	0.167924	0.056818	100.00	0.00	0.00
16	0	58	0	2.771428	0.157786	0.099151	100.00	0.00	0.00
16	2	12	0	3.2	0.151438	0.019255	100.00	0.00	0.00
16	2	23	0	2.64	0.103864	0.013258	100.00	0.00	0.00
16	2	35	0	2.854545	0.143032	0.074653	89.09	9.09	1.82
16	2	58	0.060606	3.451612	0.16825	0.178819	85.48	14.52	0.00
16	3	12	0	3.2	0.151438	0.019255	100.00	0.00	0.00
16	3	23	0	2.64	0.103864	0.013258	100.00	0.00	0.00
16	3	35	0.064516	2.844827	0.123297	0.11916	81.03	18.97	0.00
16	3	46	0.03125	3.258064	0.166441	0.143404	93.55	6.45	0.00
16	3	58	0	2.771428	0.154188	0.099151	100.00	0.00	0.00
16	5	12	0.044516	2.896551	0.189237	0.09596	72.41	27.59	0.00
16	5	23	0	2.64	0.104119	0.013258	100.00	0.00	0.00
16	5	35	0	2.869565	0.141507	0.03267	100.00	0.00	0.00
16	5	46	0.042857	3.666666	0.160513	0.42296	69.70	22.73	7.58
16	5	58	0	2.774647	0.157386	0.106096	100.00	0.00	0.00
16	6	12	0	3.2	0.151438	0.019255	100.00	0.00	0.00
16	6	23	0	2.64	0.103864	0.013258	100.00	0.00	0.00
16	6	35	0.033333	3.551724	0.139185	0.283302	87.93	10.34	1.72
16	6	46	0.015873	3.193548	0.164866	0.115688	91.94	8.06	0.00
16	6	58	0	2.771428	0.156091	0.099151	100.00	0.00	0.00
16	8	12	0.057142	2.636363	0.181889	0.144571	87.88	12.12	0.00
16	8	23	0	2.64	0.103864	0.013258	100.00	0.00	0.00
16	8	35	0.074328	3.37931	0.155394	0.156402	86.21	12.07	1.72
16	8	46	0.067142	3.101694	0.142381	0.161231	84.75	11.86	3.39
16	8	58	0.086419	3.243224	0.152286	0.286892	82.43	17.57	0.00

Table A.3: Complete results – *Deutsches Forschungsnetz* (DFN) network

<b>Deutsches Forschungsnetz (DFN) 11 node network</b>									
$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
2	0	8	0	1.5	0.055676	0.017787	100.00	0.00	0.00
2	0	15	0	1.631578	0.092703	0.029644	100.00	0.00	0.00
2	0	23	0	1.763157	0.084541	0.08498	92.11	7.89	0.00
2	0	30	0.04	1.791666	0.082405	0.169082	81.25	14.58	4.17
2	0	38	0	1.690476	0.086132	0.136957	90.48	9.52	0.00
2	1	8	0	1.5	0.055676	0.017787	100.00	0.00	0.00
2	1	15	0	1.631578	0.092703	0.029644	100.00	0.00	0.00
2	1	23	0	1.763157	0.084541	0.08498	92.11	7.89	0.00
2	1	30	0.04	1.791666	0.082405	0.169082	81.25	14.58	4.17
2	1	38	0	1.690476	0.086132	0.136957	90.48	9.52	0.00
2	2	8	0	1.5	0.055676	0.017787	100.00	0.00	0.00
2	2	15	0	1.631578	0.092116	0.029644	100.00	0.00	0.00
2	2	23	0	1.763157	0.084541	0.08498	92.11	7.89	0.00
2	2	30	0.058823	1.75	0.082538	0.183575	83.33	12.50	4.17
2	2	38	0	1.690476	0.086132	0.136957	90.48	9.52	0.00
2	3	8	0	1.5	0.055676	0.017787	100.00	0.00	0.00
2	3	15	0	1.631578	0.092665	0.029644	100.00	0.00	0.00
2	3	23	0.023809	1.878048	0.083446	0.247826	78.05	19.51	2.44
2	3	30	0.078431	1.851063	0.082517	0.209239	74.47	21.28	4.26
2	3	38	0.043478	1.704545	0.083113	0.282609	77.27	22.73	0.00
2	4	8	0	1.5	0.055676	0.017787	100.00	0.00	0.00
2	4	15	0	1.631578	0.092703	0.029644	100.00	0.00	0.00
2	4	23	0	1.763157	0.084541	0.08498	92.11	7.89	0.00
2	4	30	0.061224	2	0.088234	0.319876	63.04	28.26	8.70
2	4	38	0.021739	1.844444	0.087548	0.289855	77.78	20.00	2.22
2	5	8	0.0166666	1.8	0.051816	0.152174	80.00	20.00	0.00
2	5	15	0	1.631578	0.092703	0.029644	100.00	0.00	0.00
2	5	23	0	1.763157	0.084722	0.08498	92.11	7.89	0.00
2	5	30	0.04	1.791666	0.082405	0.169082	81.25	14.58	4.17
2	5	38	0	1.690476	0.090446	0.136957	90.48	9.52	0.00
4	0	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	0	15	0	1.631578	0.094287	0.014822	100.00	0.00	0.00
4	0	23	0	1.68421	0.087374	0.040514	100.00	0.00	0.00
4	0	30	0	1.645833	0.074959	0.072464	100.00	0.00	0.00
4	0	38	0	1.642857	0.087015	0.066304	97.62	2.38	0.00
4	1	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	1	15	0	1.631578	0.094287	0.014822	100.00	0.00	0.00
4	1	23	0	1.68421	0.087374	0.040514	100.00	0.00	0.00
4	1	30	0.020408	1.979166	0.078204	0.197464	77.08	14.58	8.33
4	1	38	0	1.642857	0.087015	0.066304	97.62	2.38	0.00
4	2	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	2	15	0	1.631578	0.094287	0.014822	100.00	0.00	0.00
4	2	23	0	1.68421	0.087374	0.040514	100.00	0.00	0.00

$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
4	2	30	0	1.645833	0.074959	0.072464	100.00	0.00	0.00
4	2	38	0.021276	1.695652	0.08466	0.154891	84.78	15.22	0.00
4	3	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	3	15	0.021739	2.071428	0.091508	0.152174	67.86	14.29	17.86
4	3	23	0	1.68421	0.087274	0.040514	100.00	0.00	0.00
4	3	30	0	1.645833	0.074959	0.072464	100.00	0.00	0.00
4	3	38	0.021739	1.688888	0.083889	0.160326	86.67	13.33	0.00
4	4	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	4	15	0.066666	2.035714	0.092684	0.128458	71.43	14.29	14.29
4	4	23	0	1.68421	0.087161	0.040514	100.00	0.00	0.00
4	4	30	0.021276	1.652173	0.075465	0.113354	93.48	6.52	0.00
4	4	38	0.021739	1.733333	0.08739	0.213315	82.22	17.78	0.00
4	5	8	0	1.5	0.056903	0.008893	100.00	0.00	0.00
4	5	15	0	1.631578	0.094289	0.014822	100.00	0.00	0.00
4	5	23	0.021739	1.666666	0.08762	0.121981	91.11	8.89	0.00
4	5	30	0	1.645833	0.074959	0.072464	100.00	0.00	0.00
4	5	38	0.078431	1.723404	0.084377	0.223602	82.98	17.02	0.00
8	0	8	0	1.5	0.059291	0.004941	100.00	0.00	0.00
8	0	15	0	1.631578	0.097499	0.01087	100.00	0.00	0.00
8	0	23	0	1.68421	0.090415	0.030632	100.00	0.00	0.00
8	0	30	0	1.645833	0.077861	0.051329	100.00	0.00	0.00
8	0	38	0	1.642857	0.090255	0.044565	100.00	0.00	0.00
8	1	8	0	1.5	0.059291	0.004941	100.00	0.00	0.00
8	1	15	0	1.631578	0.097499	0.01087	100.00	0.00	0.00
8	1	23	0	1.68421	0.090415	0.030632	100.00	0.00	0.00
8	1	30	0	1.645833	0.077861	0.051329	100.00	0.00	0.00
8	1	38	0	1.681818	0.088536	0.099864	100.00	0.00	0.00
8	2	8	0	1.5	0.059291	0.004941	100.00	0.00	0.00
8	2	15	0	1.631578	0.097499	0.01087	100.00	0.00	0.00
8	2	23	0	1.68421	0.090415	0.030632	100.00	0.00	0.00
8	2	30	0	1.653061	0.077677	0.070652	100.00	0.00	0.00
8	2	38	0.043478	1.681818	0.087604	0.150136	93.18	6.82	0.00
8	3	8	0	1.5	0.059291	0.004941	100.00	0.00	0.00
8	3	15	0.057142	2.060606	0.09446	0.210474	72.73	27.27	0.00
8	3	23	0	1.68421	0.090415	0.030632	100.00	0.00	0.00
8	3	30	0	1.630434	0.078814	0.106366	95.45	4.55	0.00
8	3	38	0.020408	1.729166	0.086081	0.134964	85.42	14.58	0.00
8	4	8	0.125	2	0.055274	0.171937	71.43	28.57	0.00
8	4	15	0.037037	2.038461	0.102768	0.128953	65.22	21.74	13.04
8	4	23	0	1.68241	0.090415	0.030632	100.00	0.00	0.00
8	4	30	0.01923	2.098039	0.075819	0.143116	80.39	19.61	0.00
8	4	38	0.021739	1.777777	0.086816	0.134783	80.00	20.00	0.00
8	5	8	0	1.5	0.059291	0.004941	100.00	0.00	0.00
8	5	15	0	1.631578	0.097499	0.01087	100.00	0.00	0.00
8	5	23	0.083333	1.977272	0.102113	0.164855	75.00	22.73	2.27
8	5	30	0	1.914893	0.081624	0.207609	89.36	10.64	0.00
8	5	38	0	1.651162	0.094455	0.131793	76.74	18.60	4.65

$\lambda$	Link failures	Traffic flows	Blocking prob.	Average hops	Ave. pkt delay	Link util.	% P1	% P2	%P3
16	0	8	0	1.5	0.064208	0.004695	100.00	0.00	0.00
16	0	15	0	1.631578	0.103825	0.009634	100.00	0.00	0.00
16	0	23	0	1.68421	0.09649	0.027915	100.00	0.00	0.00
16	0	30	0	1.645833	0.083723	0.044082	100.00	0.00	0.00
16	0	38	0	1.642857	0.096533	0.041848	100.00	0.00	0.00
16	1	8	0	1.5	0.064208	0.004694	100.00	0.00	0.00
16	1	15	0	1.631578	0.103825	0.009634	100.00	0.00	0.00
16	1	23	0	1.68421	0.09649	0.027915	100.00	0.00	0.00
16	1	30	0	1.645833	0.083723	0.044082	100.00	0.00	0.00
16	1	38	0	1.642857	0.096533	0.041848	100.00	0.00	0.00
16	2	8	0	1.5	0.064208	0.004694	100.00	0.00	0.00
16	2	15	0	1.6	0.103966	0.014081	100.00	0.00	0.00
16	2	23	0	1.68421	0.09649	0.027915	100.00	0.00	0.00
16	2	30	0	1.645833	0.083723	0.044082	100.00	0.00	0.00
16	2	38	0	1.642857	0.096533	0.041848	100.00	0.00	0.00
16	3	8	0	1.5	0.064208	0.004694	100.00	0.00	0.00
16	3	15	0	1.631578	0.102802	0.009634	100.00	0.00	0.00
16	3	23	0	1.68421	0.09649	0.027915	100.00	0.00	0.00
16	3	30	0	1.64583	0.083723	0.044082	100.00	0.00	0.00
16	3	38	0.020408	1.854166	0.11285	0.339674	68.75	31.25	0.00
16	4	8	0	1.5	0.064208	0.004694	100.00	0.00	0.00
16	4	15	0	1.631578	0.103825	0.009634	100.00	0.00	0.00
16	4	23	0.021739	1.711111	0.099741	0.060802	86.67	13.33	0.00
16	4	30	0.021276	1.913043	0.09841	0.206522	71.74	26.09	2.17
16	4	38	0.043478	1.681818	0.093823	0.146739	93.18	6.82	0.00
16	5	8	0	1.5	0.064208	0.004694	100.00	0.00	0.00
16	5	15	0	1.631578	0.103825	0.009634	100.00	0.00	0.00
16	5	23	0	1.68421	0.096263	0.027915	100.00	0.00	0.00
16	5	30	0	1.645833	0.083723	0.044082	100.00	0.00	0.00
16	5	38	0	1.642857	0.096533	0.041848	100.00	0.00	0.00

# Appendix B

## List of figures

2.1: Profile of a typical multi-strand fiber optic cable, designed for underground use .....	10
2.2: Graph of fiber attenuation versus wavelength, showing historic water peak located at 1383 nm. The 18 CWDM wavelengths are also shown .....	11
2.3: Schematic illustration of the structure of a double heterojunction stripe contact laser diode.....	12
2.4: Structures of (a) vertical p-i-n photodiode and (b) a lateral p-i-n photodiode .....	13
2.5: Schematic of avalanche photodiode (APD) .....	14
2.6: Block diagram showing typical inline amplifier configuration.....	15
2.7: Block diagram of EDFA amplification system .....	16
2.8: Diagram of symmetrical fused tapered coupler .....	17
2.9: Schematic representation of a fiber Bragg grating.....	18
2.10: Basic OADM architecture, utilising a fiber Bragg grating.....	19
2.11: Schematic of OXC, utilising $N^2$ crossbar 2x2 switches .....	19
2.12: 3D MEMS crossconnect in two different states .....	20
2.13: Scanning electron microscope image of MEMS micromirror array .....	20
2.14: Basic SONET STS-1/OC1 frame .....	21
2.15: Expected evolution of optical protocol stack over time .....	25
2.16: Expected evolution of optical protocol stack over time .....	26
2.17: The end-to-end view of a possible future optical network: the access network, the metro network, and the long-haul backbone network .....	26
3.1: A two-fiber, unidirectional, path-switched ring (two-fiber UPSR) topology with one working and one protection path .....	30
3.2: Illustration of protection process in two-fiber UPSR topology.....	30
3.3: A two-fiber, bidirectional, line-switched ring ( two-fiber BLSR).....	30



3.4: Example of a fully connected mesh topology .....	32
3.5: Example of a fully connected mesh topology .....	32
3.6: Conceptual example of a sparsely connected mesh topology .....	33
3.7: Topology of United States NSFNET: 14 nodes, 21 links, 3.0 connectivity factor .....	34
3.8: Topology of European Optical Network: 11 nodes, 24 links, 4.54 connectivity factor .....	34
3.9: Topology of the DFN-network ( <i>Deutsches Forschungsnetz</i> ) .....	36
3.10: Topology of SAT-3/WASC/SAFE undersea fiber optic cable.....	37
4.1: Two network entities (end nodes) are typically connected by switching devices that only implements the first three layers of the OSI protocol stack .....	41
4.2: Example of a typical optical network protocol stack .....	42
4.3: Survivability at IP/MPLS/WDM layers .....	42
4.4: Dijkstra's algorithm in pseudocode.....	44
4.5: APS in a path-switched ring topology that makes use of an operations, administration and maintenance (OAM) channel.....	47
4.6: Operation of APS in a four-fiber BLSR. Operation in (a) is normal operations, while (b) is after a failure has occurred .....	48
4.7: Differences between path protection (a) and link protection (b).....	50
4.8: Taxonomy of survivability with regard to protection and restoration.....	52
4.9: Process of restoration using the sender-chooser method.....	55
5.1: Screenshot of OPNET WDM Guru network simulator package.....	58
5.2: Example of NS2 OTcl script file .....	62
5.3: Screenshot of the graphical output file of the OTcl code of figure 5.2 .....	62
5.4: Screenshot of the network animator module (NAM) together with descriptions .....	63
5.5: OWns architecture and layers.....	65
5.6: OWns components organisations and interactions.....	68
6.1: The Unites States backbone network .....	70

6.2: Screenshot of the United States backbone network topology created in NS2 .....	70
6.3: The Italian backbone network .....	71
6.4: Screenshot of the Italian backbone network topology created in NS2.....	72
6.5: Topology of the DFN-network ( <i>Deutsches Forschungsnetz</i> ) .....	73
6.6: Screenshot of the DFN network topology created in NS2 .....	73
6.7: Screenshot of OWns, showing different wavelengths represented by different colours .....	75
6.8: Screenshot of OWns, showing two packets that are being tracked, with additional information about the packets being displayed .....	76
6.9: Screenshot of OWns, showing the capability of graphically displaying the traffic loads on individual links.....	77
6.10: The OTcl file taxonomy of OWns.....	78
6.11: Tcl code for creation of nodes in network topology.....	78
6.12: Segment of Tcl code (table <i>t</i> ) illustrating link creation, link delay, link orientation and link identity .....	79
6.13: Segment of Tcl code illustrating logical link creation.....	80
6.14: Segment of Tcl code illustrating link failure and restoration of service .....	81
6.15: Screenshot of OWns, showing link failure between nodes 8 and 9 .....	82
6.16: Segment of Tcl code illustrating randomization of link failures.....	83
6.17: Screenshot of OWns, showing 2 links that are down simultaneously.....	84
6.18: Flowchart of the modified path selection and new protection strategy in OWns ....	87
7.1: Blocking probability with 2 wavelengths and zero link failures.....	93
7.2: Blocking probability with 2 wavelengths and moderate number of link failures .....	94
7.3: Blocking probability with 2 wavelengths and high number of link failures .....	95
7.4: Blocking probability with 4 wavelengths and zero link failures.....	96
7.5: Blocking probability with 4 wavelengths and moderate number of link failures .....	97
7.6: Blocking probability with 4 wavelengths and high number of link failures .....	98
7.7: Blocking probability with 16 wavelengths and zero link failures.....	99
7.8: Blocking probability with 16 wavelengths and moderate number of link failures ..	100

---

7.9: Blocking probability with 16 wavelengths and high number of link failures .....	101
7.10: Average overall blocking probability for all 360 simulation scenarios .....	102
7.11: Usage of path 1 with increasing number of available wavelengths .....	104
7.12: Usage of path 2 with increasing number of available wavelengths .....	105
7.13: Usage of path 3 with increasing number of available wavelengths .....	106
7.14: Link utilization with increasing number of available wavelengths.....	107

# Appendix C

## List of tables

1.1: DWDM (ITU-T G. 694.1) frequency spacing grid .....	3
1.2: CWDM (ITU-T G. 694.2) wavelength spacing grid .....	4
2.1: Commonly used SONET and SDH transmission rates .....	22
3.1: Comparison of graph theory and optical network terminology .....	28
4.1: The 7-layer OSI protocol stack .....	40
6.1: Comparison between the United States backbone network, the Italian backbone network and the DFN .....	74
6.2: Network simulation topology parameters – wavelengths .....	89
6.3: Network simulation topology parameters – link failures .....	90
6.4: Network simulation topology parameters – traffic flows.....	91
7.1: Blocking probability with 2 wavelengths and zero link failures.....	93
7.2: Blocking probability with 2 wavelengths and moderate number of link failures .....	94
7.3: Blocking probability with 2 wavelengths and high number of link failures .....	95
7.4: Blocking probability with 4 wavelengths and zero link failures.....	96
7.5: Blocking probability with 4 wavelengths and moderate number of link failures .....	97
7.6: Blocking probability with 4 wavelengths and high number of link failures .....	98
7.7: Blocking probability with 16 wavelengths and zero link failures.....	99
7.8: Blocking probability with 16 wavelengths and moderate number of link failures ..	100
7.9: Blocking probability with 16 wavelengths and high number of link failures .....	101
7.10: Average overall blocking probability for all 360 simulation scenarios .....	102

---

7.11: Usage of path 1 with increasing number of available wavelengths .....	104
7.12: Usage of path 2 with increasing number of available wavelengths .....	105
7.13: Usage of path 3 with increasing number of available wavelengths .....	106
7.14: Link utilization with increasing number of available wavelengths.....	107
A.1: Complete results – United States backbone network .....	121
A.2: Complete results – Italian backbone network.....	124
A.3: Complete results – <i>Deutsches Forschungsnetz</i> (DFN) network.....	127