Survivability and Resilience Mechanisms in modern Optical Fibre Systems

by

TILANA VAN DER WESTHUIZEN

99047030

Submitted in partial fulfilment of the requirements for the degree of Master of Engineering
in the
Department of Electrical, Electronic and Computer Engineering
University of Pretoria

October 2005

I, _____ student number _____ hereby declare that all work described in this dissertation is my own, except where explicitly indicated otherwise.

Wherever I have used information from other sources, I have given credit by proper and complete referencing of the source material so that it can be clearly discerned what is my own work and what was quoted from other sources. I acknowledge that failure to comply with the instructions regarding referencing will be regarded as plagiarism. If there is any doubt about the authenticity of my work, I am willing to attend an oral ancillary examination/evaluation of the work.

SUMMARY

Title: Survivability and Resilience Mechanisms in modern Optical Fibre Systems

Candidate: T van der Westhuizen
99047030

Supervisor: Prof. F.W. Leuschner

Department: Department of Electrical, Electronic and Computer Engineering
University of Pretoria

Degree: Masters in Computer Engineering

Optical fibre networks play an increasingly prominent role in communications. As networks grow in size and complexity, the probability and impact of failures increase. In this dissertation, different optical network concepts, survivability and resilience methods are considered.

Link and Path failures are discussed and Static Path Protection (SPP), Shared Backup Path Protection (SBPP), as well as Path Restoration (PR) are investigated. A Shared Backup Path Protection model and simulation tool is designed and implemented. This implementation is compared with other studies. Dual-link failures are considered under specific network topologies. Shortest Path algorithms are used to reprovision optimal routes for backup protection.

Results and conclusions are discussed in detail, giving valuable insight into resilience methods. Availability and protectability are discussed and evaluated as measures of resilience and network survivability. Results vary between compromising little availability and bringing a significant improvement in availability.

It is concluded that the implementation of SBPP is a necessity in highly-meshed networks with high availability needs, but doesn't necessarily provide the best solution for sparsely-connected networks. The additional cost involved in the implementation needs to be considered carefully.

Keywords: Resilience, Shortest Path Algorithms, Survivability, Optical Networks, Restoration, Double Link failures, Protection, Shared Backup Path Protection, Mesh Networks.

ACKNOWLEDGMENTS

My thanks to the following people for their support:

- My fiancé, Stefan, for all the pressure and encouragement.
- Prof. Leuschner, for his guidance.
- My manager, Marianne, for the voluntary backing.
- Many thanks to my student friends in the same situation, who offered help and support wherever they could.

LIST OF ABBREVIATIONS

APS - Automatic Protection Switching

ASON - Automatic Switched Optical Network

ATM - Asynchronous Transfer Mode

BLSR - Bidirectional Line Switched Ring

CPU - Central Processing Unit

DWDM - Dense Wavelength Division Multiplexing

FTTH - Fibre to the Home

FTTC - Fibre to the Curb

Gbps - Gigabits per second

ION - Intelligent Optical Networks

IP - Internet Protocol

IS-IS - Intermediate System-to-Intermediate System

MTBF - Mean time between failures

MTTR - Mean time to repair

OSPF - Open Shortest Path First

OXS - Optical Cross Connect

PC - Personal Computer

PR - Path restoration

PVC - Polyvinyl chloride

QoS - Quality of Service

RPR - Resilient Packet Ring

SBPP - Shared Backup Path Protection

SDH - Synchronous Digital Hierarchy

SHR - Self-healing Ring

SNO - Second Network Operator

SPP - Static Path Protection

SPT - Shortest Path Tree

SONET - Synchronous Optical Network

UPSR - Unidirectional Path Switched Ring

CONTENTS

CHAPTER 1: INTRODUCTION 9

1.1 OVERVIEW 9
1.2 MOTIVATION 9
1.3 PROBLEM STATEMENT 9
1.4 APPROACH 10
1.5 OBJECTIVES 10
1.6 CONTRIBUTION 11
1.7 DOCUMENT LAYOUT 11

CHAPTER 2: BACKGROUND THEORY 12

2.1 INTRODUCTION 12
2.2 THEORETICAL CONCEPTS 13

CHAPTER 3: CONSIDERATIONS AND ASSUMPTIONS 25

3.1 SURVIVABILITY CONSIDERATIONS 25
3.2 ASSUMPTIONS 26
3.3 CRITERIA FOR MEASURING RESILIENCE MECHANISMS 28

CHAPTER 4: EXPERIMENTAL METHODOLOGY AND APPROACH 32

4.1 INTRODUCTION 32
4.2 NETWORK TOPOLOGY AND TRAFFIC MODEL 34
4.3 NETWORK SIMULATION 39
4.3.1 Input Variables: 39
4.4 RESTORATION SIMULATION 39
4.4.1 Link Matrix 39
4.4.2 Algorithm 40
4.4.3 Shortest Path Algorithm 41
4.5 DESIGN TOOLS AND METHODOLOGY 45
4.6 FUNCTIONAL ANALYSIS 45
4.7 SYSTEM SPECIFICATIONS 45

4.9 SYSTEM FLOW DIAGRAM 45

CHAPTER 5: SIMULATION TEST RESULTS 45

5.1 INTRODUCTION 45

5.2 STATIC PATH PROTECTION 45

5.3 SHARED BACKUP PATH PROTECTION 45

5.3.1 Test network simulation – parameters, assumptions and results 45

5.3.2 Simulation results 45

5.3.3 PAN-European network simulation – parameters, assumptions and results 45

5.3.4 Explanation and analysis of results 45

CHAPTER 6: CONCLUSION 45

6.1 INTRODUCTION 45

6.2 SUMMARY 45

6.3 ASSESSMENT OF STUDY 45

6.3 RECOMMENDATION FOR FUTURE WORK 45

REFERENCES 45

APPENDIX 1: ADDITIONAL READING MATERIAL 45

APPENDIX 2: EXPERIMENTAL DATA 45

APPENDIX 3: LIST OF DEFINITIONS 45

CHAPTER 1: INTRODUCTION

1.1 OVERVIEW

Optical fibre networks play a more prominent role in communications than ever before. In this document, concepts about optical networks are discussed, with specific reference to optimisation and resilience in modern optical fibre networks. Different optimisation methods are investigated and development and simulations are done on certain methods in order to ascertain the value of optimisation and protection in optical fibre networks.

1.2 MOTIVATION

Network survivability is an issue of great concern to a telecommunications industry eager to deploy high-capacity fibre networks. Loss of services in high-capacity fibre systems due to disasters and catastrophic failures could be devastating and result in significant revenue losses and unacceptable quality of service (QoS) levels.

1.3 PROBLEM STATEMENT

The problem addressed in this project is one of optimisation of resilience algorithms for specific network applications. Backbone networks between cities are critical components in ensuring connectivity and intercity communications. Backbone network protection is a challenge, since the connectivity between nodes is not necessarily very high. Whether resilience algorithms can bring a productive and economic improvement on this type of network remains to be proven.

The next big step in the evolution of optical networks is surely moving to Intelligent Optical Networks (ION), using optical switching nodes and built-in intelligence for dynamic connection configuration, network optimisation and restoration [1].

The technical challenge of the project includes:

- The use of optimisation and resilience mechanisms, which is an important factor in optical network performance.
- The implementation of different strategies in network resilience, the decision of the best algorithms to implement and the enhancement of existing strategies to produce encouraging results.

1.4 APPROACH

The aim of this research dissertation is the investigation of network resilience mechanisms. This is accomplished by a literature study and simulation. Current network restoration algorithms are analysed and the performance thereof compared. A specific focus is put on shortest route algorithms, with the aim to find a more time-effective and robust solution. Dedicated path protection, shared path protection and link protection are also investigated. Experimentation is done and statistical comparisons drawn between different solutions, using a number of criteria. The challenge is to manage shared restoration capacity, while achieving timely and reliable failure analysis and protection.

1.5 OBJECTIVES

The objectives of the dissertation are as follows:

- Simulation of an optical network, using the network topology discussed in later sections.
- Evaluation of traffic models for medium- and long-term demand.
- Estimation of link capacity requirements.
- Implementation of shortest route algorithms and survivability mechanisms on the network.
- Assessment and evaluation of network performance: availability, protectability, etc.

1.6 CONTRIBUTION

The contribution made to the optical network study field includes:

- The design and implementation of a simulation tool for SBPP.
- The comparison of different network topologies.
- The use of an alternative and more optimal shortest path algorithm called Nicholson's algorithm.
- Optimising weight design by incorporating capacity and distance parameters.

1.7 DOCUMENT LAYOUT

This document is structured as follows:

- **Chapter 2** contains theoretical concepts of importance in this study.
- **Chapter 3** highlights assumptions, considerations and different evaluation criteria.
- **Chapter 4** explains the network and traffic model, presents a functional breakdown and stipulates deliverables for this project.
- **Chapter 5** discusses the implementation and simulation process of different algorithms experimented on. Evaluation of results is also included in this chapter.
- The document is concluded in **Chapter 6**.
- **References** are given at the end of the document.
- **Appendix 1, 2 and 3** contain additional reading material, experimental data and a list of definitions.

CHAPTER 2: BACKGROUND THEORY

2.1 INTRODUCTION

In the late 1980s we witnessed the first deployment of optical networks. Today we see the proliferation of data and storage networks. Standardisation of Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), as well as the high-speed optical interfaces on other devices, such as Internet Protocol (IP) routers and Asynchronous Transfer Mode (ATM) switches, also prompted the use of innovative architectures for optical networks [2].

Wavelength routing networks became a major focus in the early 1990s as people realised the benefits of having an optical layer which is capable of performing switching and routing in a more economical way. The optical network is currently evolving to provide additional functionality, including the ability to set up and take down light paths in a dynamic approach, optimal rerouting of light paths and the restoration of light paths in the case of a network failure [3]. A combination of these factors is resulting in the introduction of intelligent optical ring and mesh networks [4].

The concepts of fibre to the home (FTTH) and curb (FTTC) are major promoters for optical networks, as Internet and communication become easily accessible and inexpensive to all walks of life. The high infrastructure cost limitations that have been overcome due to telecommunication deregulation in most first world countries, as well as the increasing need for broadband services, heighten the need for better networks. In South Africa specifically, the inevitable deployment of a second network operator, or SNO, necessitates the use of state-of-the-art technology.

In order to provide high quality communication services to clients, survivability is a crucial concern in any commercial communications network [5]. It can be approached mainly in two ways: protection and restoration. With the former, failure recovery is pre-provisioned; the latter involves more dynamic signal recovery. Protection schemes have two forms: in one, traffic is

transmitted over both the primary path and a (pre-provisioned) secondary path, or protection, and the end point chooses between them on the basis of signal quality. In the other approach, a secondary path is predetermined, which can be used by low-priority traffic until it is needed to protect the primary path. Additionally, different levels of protection granularity can also be provisioned: at the fibre level, the wavelength level, etc. Unlike protection approaches, restoration schemes use rerouting. They calculate the secondary path and set it up only after failure has occurred. Restoration is therefore slower than protection, for which SONET has established a benchmark time of 50 ms [6]. In both approaches, obviously, prompt detection and notification of failures are critical for fast failure recovery and reliable networks. These theoretical terms and more are discussed in more detail in the next section.

2.2 THEORETICAL CONCEPTS

2.2.1 Protection vs. Restoration

The distinction between protection and restoration is not always well-defined, but for the purpose of this document the following distinction is made: protection is considered the technique used in optical networks where failure paths are already computed on outset. This is inflexible, but a very fast way of correcting network problems. Restoration is a term used for a strategy that computes alternative paths at the time of failure, taking into consideration the status of the network on that specific instance and the bandwidth and resources available in the network. This technique needs additional signalling and is therefore more time-consuming, but provides optimal results.

In order to make networks survivable, most protection techniques involve some redundant capacity within the network and rerouting of traffic after a failure, using the spare capacity. Most failures in the network are as a result of link failures (cables being cut), failure of active components (e.g. transmitters/receivers), or node failures [7]. According to Demeester [8], cable cuts are related to link length and typically vary between 50 and 200 days per 1000 km. The restoration times required depend on the application/type of data being transmitted. Signalling is also required on the network to facilitate switching between normal and redundant capacity.

2.2.2 Protection concepts

- *Working or primary paths* carry traffic under normal operation, while *protection or secondary paths* are used in failure situations to provide an alternative path [7].
- Protection is *dedicated* when the working paths and protection paths are replicas of each other, while *shared* protection shares protection paths between working paths.
- *Revertive* protection schemes automatically change traffic back to working paths when a failure has been corrected. In *non-revertive* schemes, traffic needs to be moved manually.
- Protection switching can also be *unidirectional* or *bi-directional*. After a unidirectional fibre cut, both directions of traffic are switched over to the protection fibres, instead of only the affected direction of traffic. During bi-directional switching, the receiver needs to inform the sender of the failure, using a signalling protocol called automatic protection switching (APS), before switching occur.

2.2.3 WDM, DWDM, etc.

Optical fibres employing the technique of wavelength division multiplexing (WDM) can support around 1000 times the capacity of their electronic counterparts [6]. WDM allows the simultaneous transmission of several channels on the same fibre, each on a different wavelength (frequency). WDM is deployed in commercial point-to-point fibre links, including undersea installations. WDM-based optical networks are continually tested and implemented in the U.S. (e.g., MONET, NTONC projects) [9] and Europe (RACE, ACTS projects) [10].

This technique has been extended to Dense Wavelength Division Multiplexing (DWDM), which increases the capacity of embedded fibre by spacing the wavelengths more closely than does WDM and therefore has a higher overall capacity. DWDM terminals carry up to 80 wavelengths, a total of 200 Gigabits per second (Gbps), or up to 40 wavelengths, a total of 400 Gbps—which is enough capacity to transmit 90,000 volumes of an encyclopaedia in one second [A1]. This is necessary to accommodate for the explosion in demand for network bandwidth, which as a result of data-centric traffic, is increasing rapidly.

A number of WDM network simulation tools are available in the literature for experimentation purposes [11].

2.2.4 Ring vs. Mesh Networks

One way to survive an optical network failure is to duplicate transmission paths. Rings are used as an approach and is the most widely-spread solution in use today [12]. It has long been the view that this is an inefficient approach, although it has to be admitted that rings did come in handy when survivability issues reached crisis proportions in the 1990s. In light of the expansion and popularity of optical networks, it became necessary to have networks that are survivable, but also more flexible, scalable, able to accommodate different services and far more efficient in the use of capacity. This is where mesh networks are effectively utilised [13]. Mesh restoration is said to require considerably less redundant capacity than rings, while providing full restoration against any single failure scenario [14]. Multiple studies have been conducted on protection and restoration of mesh topological structures [15], [16], [17], [18], [19]. Due to practical limitations, paths often share the same cable or duct, for example a bridge crossing. Mesh – Ring combinations are therefore also utilised. **Figure 2.1: Ring and Mesh Networks** shows a graphical representation of ring and mesh networks.

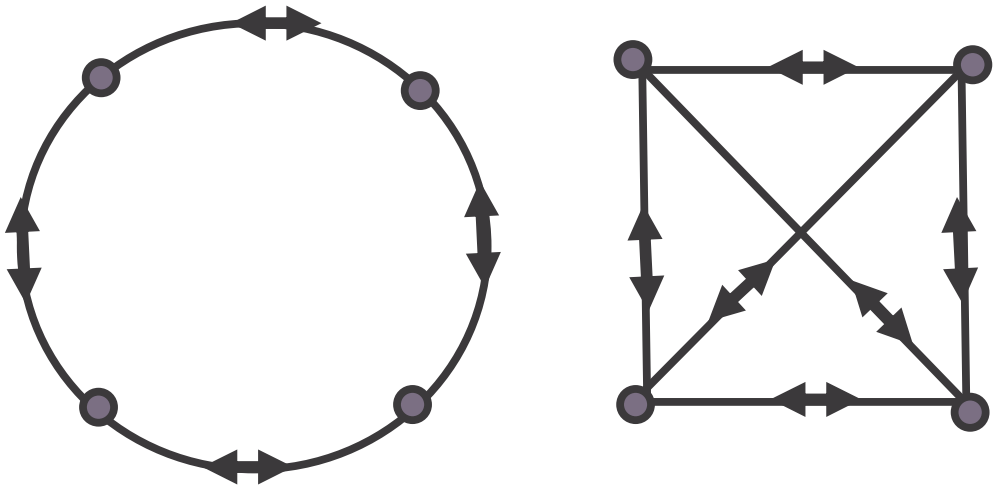


Figure 2.1: Ring and Mesh Networks

2.2.5 Layered Protection

Survivability can be addressed at various layers in the network. The reason for protection at different layers is that each layer will be able to protect effectively against certain types of failures [20]. Each layer's resilience method provides a service to the higher layer.

2.2.6 Physical Layered Protection

The physical layer protection enhances the physical protection of cables and equipment. This includes the use of Polyvinyl Chloride (PVC) ducts in protecting buried cables, the use of rodent-repelling cable sheets, as well as not marking aerial cables to reduce vandalism and theft. Deep-sea cables stand a chance to be damaged by ships' anchors and shark bites and are encased in heavily-armoured outer layers. One of the most important physical layer topological considerations is that higher layers can only restore a failure by rerouting the affected connection over a physically diverse (fully disjoint) or span-disjoint path. This effectively means that another path, which was not affected by the failure, should be available. **Figure 2.2: Explanation of disjoint and distinct routes as depicted by W. D. Grover in [13]**, explains the difference between fully disjoint, span-disjoint and distinct routes.

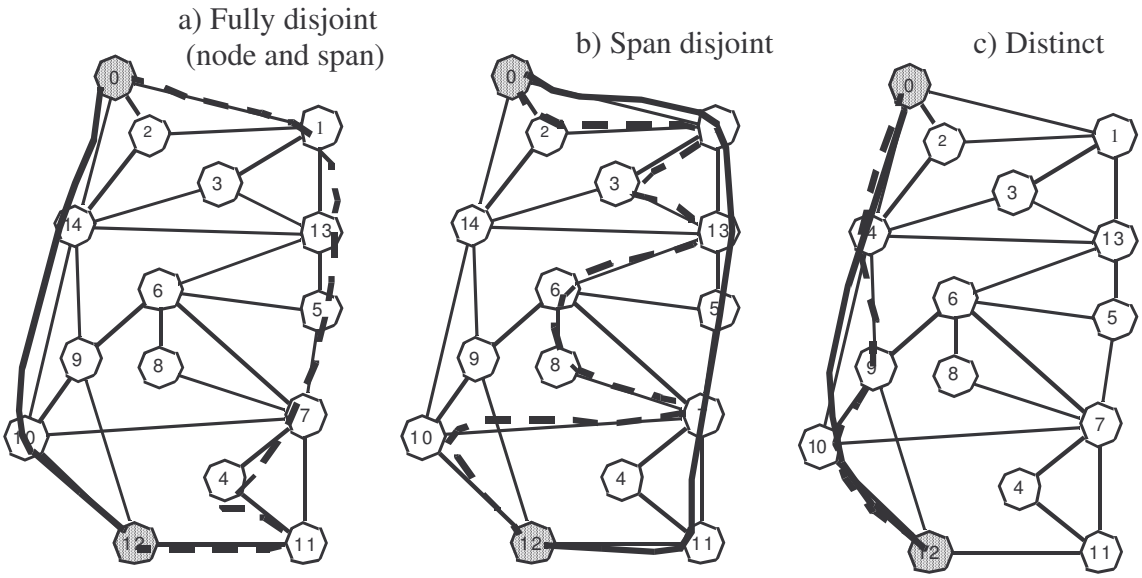


Figure 2.2: Explanation of disjoint and distinct routes as depicted by W. D. Grover in [13]

2.2.7 System Layer Protection

Transmission system survivability is mostly achieved by built-in equipment redundancy, including dual-power connections and converters and additional fibre links. The methods involved include linear Automatic Protection Switching (APS) schemes, ring schemes and p-cycles techniques. System layer survivability techniques are essentially protection schemes.

The most basic protection mechanisms used in point-to-point links are 1+1 protection, where the signal is simultaneously transmitted over the working path and protection path and the receiver chooses the better of the two, and 1:1 or 1:N protection [3]. With 1:1, the signal is transmitted only over the protection path when a failure occurs, and shared between working paths in the case of 1:N. Although 1+1 protection is a very fast mechanism and needs no signalling, 1:N has the advantage that the protection fibre is not normally used to carry primary traffic and is therefore available to carry low-priority traffic. This offers better use of spare capacity, since protection fibres can be shared between a number of working fibres. M:N protection is a variation of 1:N protection, where N protection fibres are shared between M working paths.

A ring is used to provide two disjoint paths between nodes in a network. This is a useful concept in survivability design. These are incorporated in SONET/SDH architectures to provide mechanisms to reroute traffic from failed links, and therefore the term self-healing rings (SHRs). Self-healing rings can be divided into bidirectional and unidirectional. A SHR is unidirectional if both directions of a duplex channel travel over the same path, and bidirectional if the directions follow opposite paths.

Unidirectional Path-Switched Rings (UPSRs) can be implemented using two or four fibres. One fibre/pair is used as working fibre and the other as protection. This is essentially incorporating a 1+1 scheme in a network structure. Bidirectional Line Switched Rings (BLSRs) are more sophisticated and incorporate a 1:1 protection mechanism. The protection ring is idle, or contains low-priority traffic when there are no failures. When a particular node fails, the two adjacent nodes to the failed one loop the traffic back to the protection ring.

Additional transmission layer resilience methods include Resilient Packet Rings (RPR), ring covers, loopback networks and p-cycles.

2.2.8 Logical layer survivability

The static nature of system-layered protection is overcome in the logical layer. Paths are created on demand between desired end points, using a general inventory of uncommitted logical channels, which provides features not provided by ring or APS schemes. The most important feature is higher capacity efficiency, which is provided by mesh restoration schemes permitting extensive sharing of potential capacity, as well as the management of finer granularity when manipulating wavelengths instead of whole fibre links.

Restoration, as explained earlier in the section, is used to restore traffic after a failure occurred. It is important to use the best possible route for lost traffic that must be restored. The Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) routing protocols widely-used in today's Internet compute a shortest path tree (SPT) from each router to other routers in a routing area [21]. Many existing commercial routers recompute a SPT from scratch, following changes in the link states of the network and using well-known algorithms, e.g. Dijkstra's shortest path algorithm. Such recomputation is inefficient and may consume a considerable amount of CPU time, but is still in use. Dynamic algorithms and various strategies to improve restoration exist.

It is important to understand that the best possible arrangement for survivability may be the combination of a distributed restoration mechanism embedded in the logical layer. It self-generates efficient pre-planned mesh network protection to withstand any first failure and then executes and provides best-effort state adaptive restoration to a second failure, should it arise.

Additional logical resilience mechanisms include p-cycles, meta-mesh and short leap shared protection.

The concept behind p-cycles is the formation of cyclic pre-connected or pre-configured closed paths of spare capacity. The working paths follow the shortest possible route over primary capacity. These p-cycles are formed in advance of any failure occurrence. The switching required when a failure occurs is pre-planned and essentially the same as the procedure used with rings. The difference is that the p-cycle doesn't cover the entire graph, but can protect both on-cycle and straddling, or off-cycle, failures.

2.2.9 Service layer survivability

Service layer techniques are the last defence before physical failures become apparent to the user application and are normally software-based implementation utilising virtual connections. Dynamic routing in circuit-switched networks and link-state adaptive routing schemes are the most traditional service layer schemes.

2.2.10 Path and Link restoration

Path restoration (PR) involves computing an entirely new route between start and end points of a route, while link- or span restoration computes new routes only between the nodes adjacent (nodes directly connected by a 1-hop route in the network) to the part of the network where the failure has occurred. A link is a single unit of bandwidth at the respective level of transport management.

Path restoration is more capacity- and cost-effective and, under normal conditions, provides more optimal routes than link restoration, but is more time-consuming to compute. Link- or span restoration often results in what is called loopbacks, which can be seen in **Figure 2.3: Diagrammatic representation of a loopback reaction occurring in span protection**.

2.2.11 Network control

A centralised control unit can be used to enforce control on a network. The central control unit of the control plane is aware of everything that is going on in the network. Distributed control is the other alternative where up-to-date knowledge of the network state is not known to any node. A node uses signalling to enquire about network status and routing options [22].

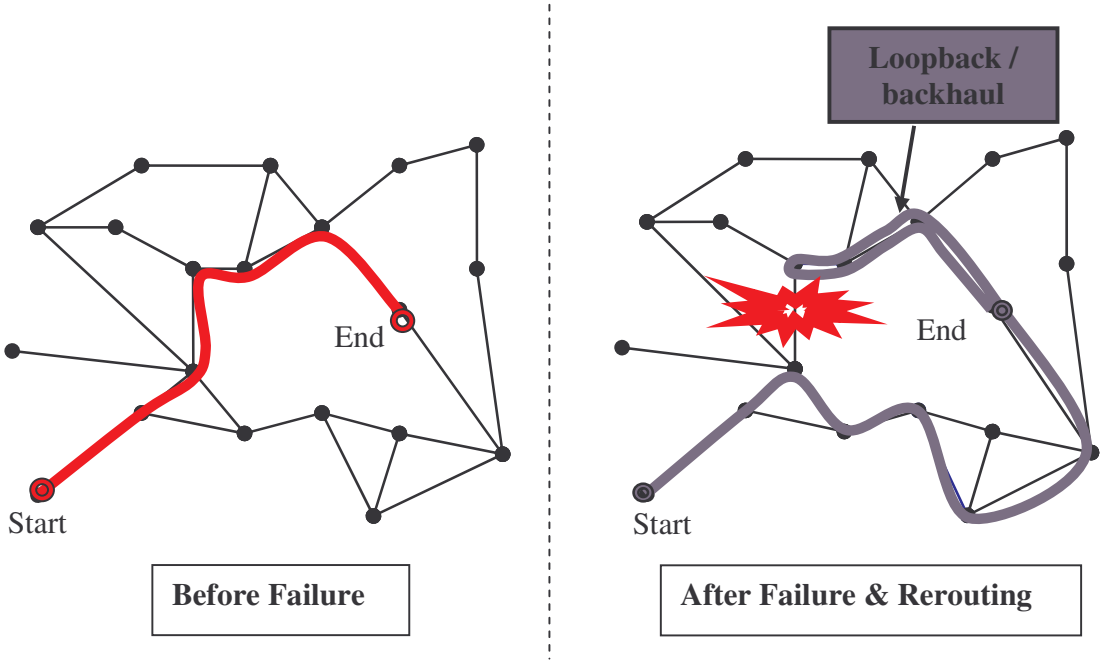


Figure 2.3: Diagrammatic representation of a loopback reaction occurring in span protection

Three basic distinctions are made between end-to-end path protection/restoration:

Static Path Protection (SPP)

- A static path table is set up in advance.
- Independent re-provisioning attempts are made.
- No co-ordination, self-organisation, or other way to address the mutual capacity considerations are implemented.
- This method is inherently unassured, a best-efforts method with unpredictable outcomes.
- Movement away from static design due to high traffic demands and effect of failure on communications have been the trend in recent years.

Shared Backup Path Protection (SBPP)

- Each working path has a (single) fully-disjoint backup route pre-determined at path-provisioning time. **Figure 2.4: Diagrammatic representation of SBPP**, depicts the working of shared backup path protection.
- When needed, a protection path is cross-connected from spare channels along the backup route.
- It is like "1+1 APS with a shared backup".
- The same end-node activated reaction occurs, regardless of where failure occurs on the working path.
- This is the most dominant current trend for "survivable routing".
- It has a high dependency on conventional software and databases.
- The advantage in fully-optical networks is that we don't need rapid fault location.

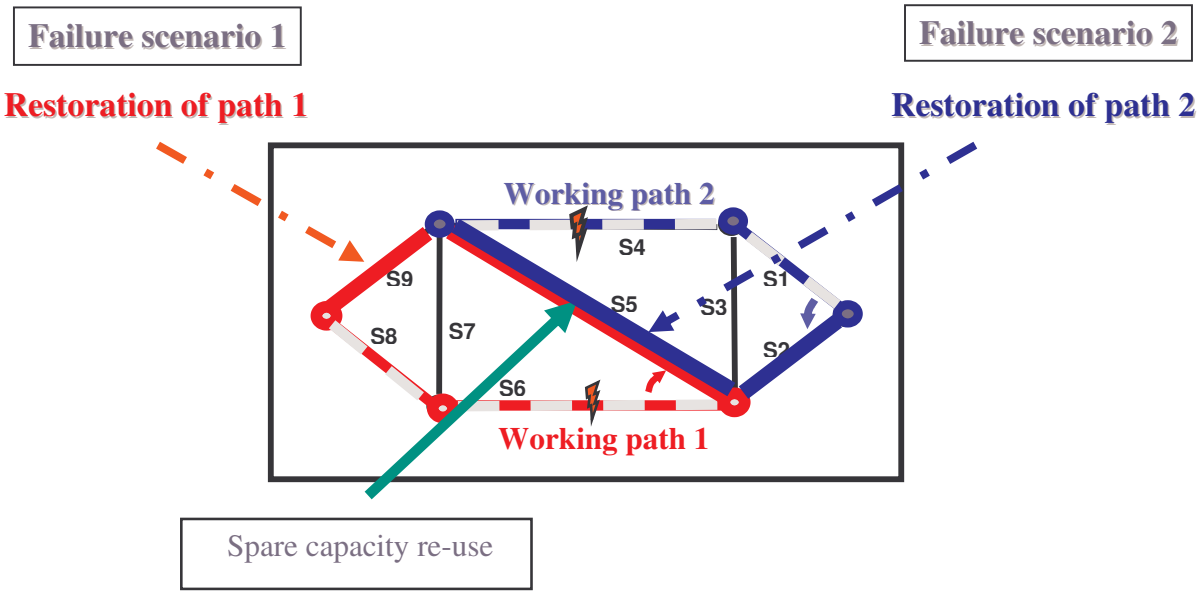


Figure 2.4: Diagrammatic representation of SBPP

("True") Path Restoration (PR)

- This has an adaptive, failure-specific response to failure and network state.
- For each failure scenario, the set of affected end-nodes are simultaneously restored.
- Allows reuse of the working capacity on the surviving portion of failed paths.
- Capacity design is necessary *to assure 100% restorability* to all defined scenarios.
- Theoretically the most efficient possible scheme [23].
- It is, however, not currently popular with industry, due to perceived complexity.
- It may return to importance in context of adaptive-second line of defence strategy for ultra-high availability, or, for maximal recovery from arbitrary-attack failure scenarios (September 11, etc.).
- True self-organisation concepts are currently *too different* from conventional software/ messaging paradigms for "distributed interaction".

2.2.12 Nodal degree

The nodal degree of a node depicts the number of links connecting the node to other nodes. The significance of this in network failure scenarios is that for a node with a nodal degree of two, only one possible path will be available if one of the links fail. A node with a nodal degree of two can effectively only protect against a single-link failure. For protection against dual link failures, nodes ideally need to have a nodal degree of at least three. The nodal degree also plays a role in determining the capacity benefit in path restoration above span restoration, as can be seen in **Figure 2.5: Nodal degrees and impact on path protection as shown by Grover [13]**. Capacity wise, a chain network can do no better with path protection than with span protection.

Recent findings indicate that the capacity benefit of path restoration (over span restoration) may be considerably less than hoped for, *in low degree networks*.

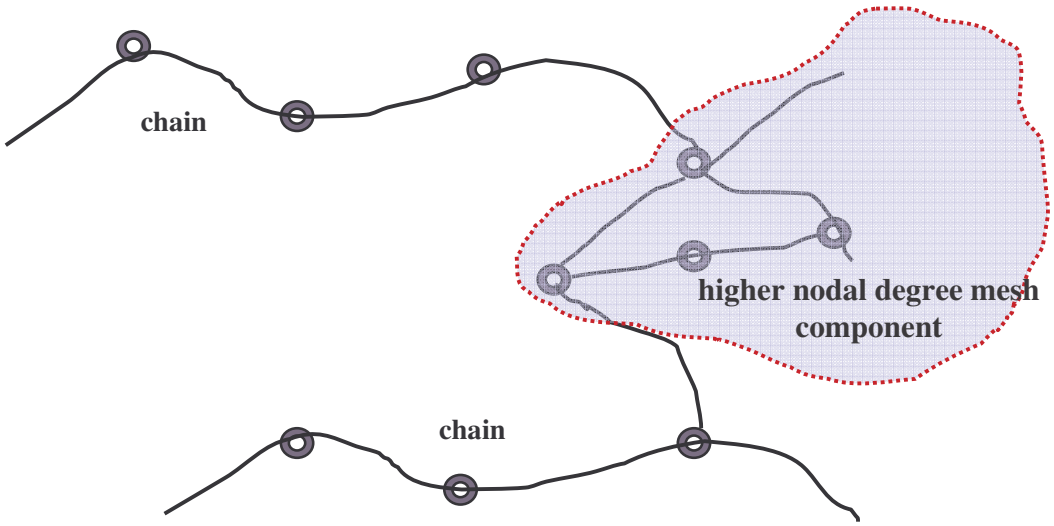


Figure 2.5: Nodal degrees and impact on path protection as shown by Grover [13]

2.2.13 Joint or non-joint design

According to Grover [13], who considers capacity and topology design for shared backup path protection, the increase in capacity needed to accommodate non-joint capacity optimisation is negligible in path protection, but not in span- or link protection optimisation. Joint capacity optimisation is used when both working and protection capacity is optimised when a failure occurs. This can be seen in **Figure 2.6: Comparison between joint and non-joint optimisation as depicted by Grover [13].**

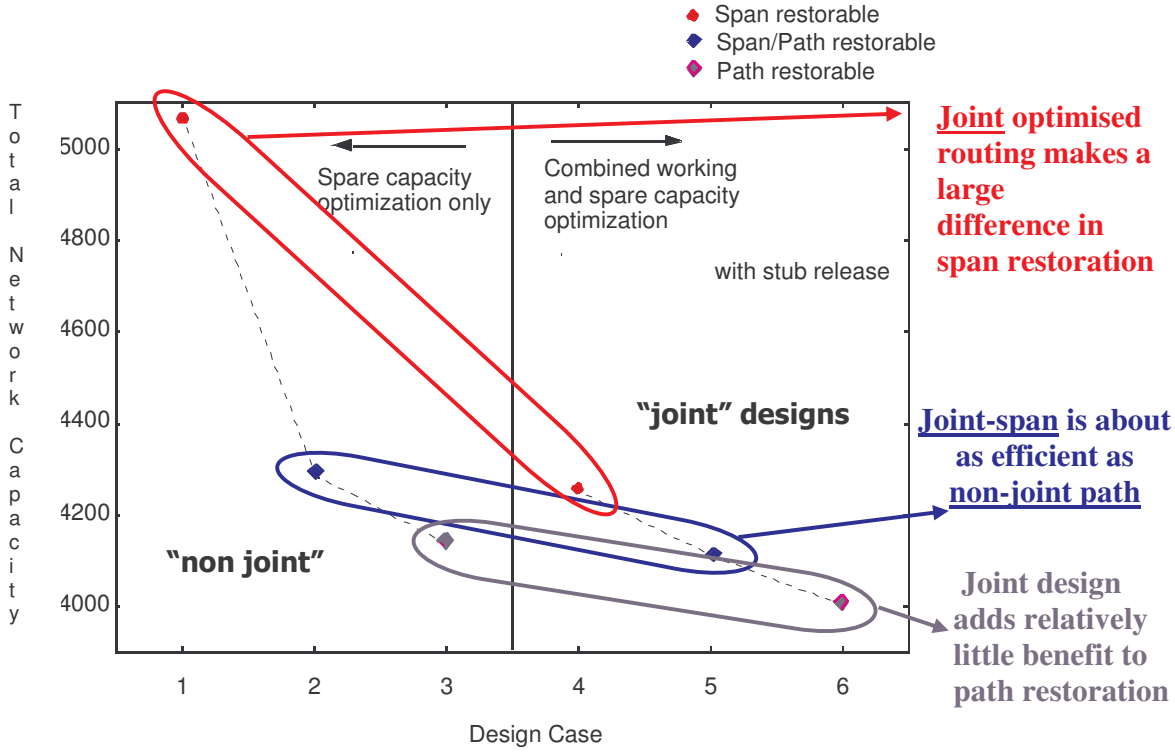


Figure 2.6: Comparison between joint and non-joint optimisation as depicted by Grover [13]

2.2.14 Stub release

Stub release is an option available to path restoration (not span restoration). This allows the release of capacity used on a route that has a link failure. Due to the failure of a node/link, the path becomes unavailable, but the unaffected links and their capacity can be reused when new paths are computed [24]. From a *capacity design* standpoint it is preferable to have stub-release. From *an operational viewpoint,* stub release complicates things. After physical repair, the reversion process is more complex, and in certain scenarios impossible [13].

CHAPTER 3: CONSIDERATIONS AND ASSUMPTIONS

3.1 SURVIVABILITY CONSIDERATIONS

There are numerous strategies that can be implemented to improve network reliability. The challenge is to choose the best combinations of these and to deploy them to create an optimal solution. Some of the most frequently-used measures are listed below:

1. Preventing failures as much as possible by performing preventative actions to most frequently-occurring faults, e.g. placing cables deeper under the ground or putting them in stronger casings to minimise cable cuts.
2. Quicker detection of failures by the use of smoke warning systems and alarms in control rooms.
3. Duplication of network links and components for critical connections.
4. Using expanded networks, e.g. mesh networks, to increase the number of paths into and out of a component – called dual homing.
5. Network recovery or resilience schemes, to automatically divert traffic to another fault-free link on the network, in case of a failure [25].

Considerations when using one or more of the above-mentioned mechanisms to improve network reliability are the following:

- **Will the method provide the necessary Quality of Service (QoS) required?**
  QoS can be presented by a number/percentage, e.g. the network availability, but other factors have to be considered. Frequency and duration of outages, as well as the immeasurable parameters such as the perceived impact of the failure on users, are some of the other factors that need to be taken into account when QoS is quantified.
- **What will the cost implication be?**
  In case of duplication of links (mechanism 5 above) or network recovery schemes, additional bandwidth must be provided to account for the traffic being diverted.
- **What is the maximum propagation delay allowed for a specific type of application?**
  This is again applicable to mechanism 5 above.

More considerations when implementing a network resilience mechanism:

- Single or multiple failures
- Distributed or centralised control
- Network layer employed on
- Single layer vs. multi layer protection
- Type of protection variant used
- Pre-planned vs. dynamic recovery routes
- Dedicated vs. shared protection
- Network technology implemented
- Path or link protection

As indicated, deciding on the correct method of network availability measures is no trivial task.

3.2 ASSUMPTIONS

3.2.1 Single vs. double link failures

The most frequent network failures that occur are either a link (cable cut between two nodes, etc.), or a node failure (component, e.g. router hardware or software failure) [26]. In most scenarios the failure of a network link or component is statistically independent of another failure in the network. Under normal network conditions the mean time to repair (MTTR) is much shorter than the mean time between failures (MTBF), therefore the probability that more than one link or node failure occurs during the same time period can be neglected. As networks grow in size, however, both the probability and impact of double-link failures increase [27]. If this is a consideration, extra measures need to be taken, since pre-allocated bandwidth cannot provide 100% protection. **Double-link failures will be considered in this study. In this analysis nodes are assumed to be failure-free and only link failures are considered.**

3.2.2 Poisson distribution

Simulation is used to model blocking probability in the protected network, where light path arrivals and departures are modelled as independent memoryless Poisson Processes. This means

that each connection is not in any way affected by the previous or next connection. Poisson arrival processes have static mean values that completely categorise the demand between two nodes, indirectly assuming a traffic prediction as accurate as in static demand cases. This is compared to a quantitative traffic model based on population growth and trends.

3.2.3.Wavelength conversion

Full wavelength conversion is assumed. The reason why this can be assumed without loss of generality is that cost and basic architectural efficiencies do not depend on the detailed channel assignment, as long as a suitable channel assignment is feasible under the capacity available. The cost of wavelength conversion is also decreasing and it will therefore be more generally implemented.

3.2.4 Failure duration

A maximum allowed restoration requirement is set at 1 to 2 seconds, recognising that there is no real effect on services up to that time [28]. This is never exceeded in the simulation results however, due to the simplified network model and switching and control activities not modelled, and can safely be neglected.

3.2.5 Failure rate

A constant failure rate is assumed for this dissertation. This is supported by the fact that external hazard factors that lead to failures are unsynchronised with the deployment of equipment and can be modelled as a constant average. Furthermore, this assumption does not affect the outcome of comparative measurements if the same assumption is used over all tests.

3.2.6 Network Topology

An undirected graph is assumed in this study, which means that links are bidirectional, with equal capacity on both directions on a link. The graph is also assumed to be planar, having links that have no intersecting points other than at nodes, which is typical of real-life physical networks. **Figure 3.1: Planar Graph**, gives an example of a typical planar graph, which, incidentally, is also the test network.

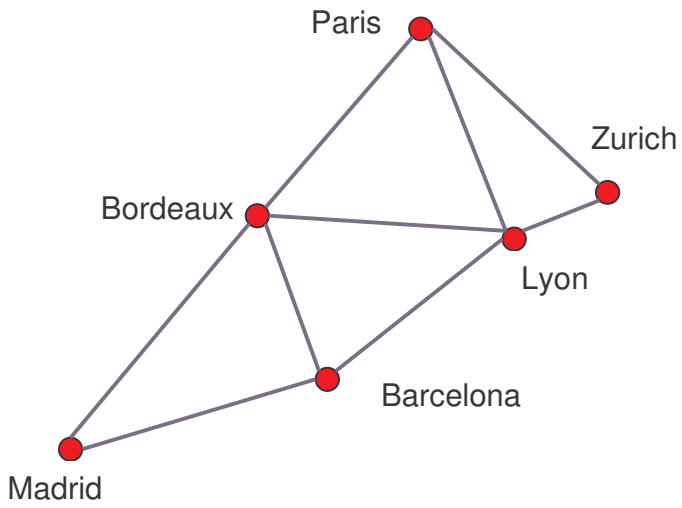


Figure 3.1: Planar Graph – Derived from Figure 4.3

It should be noted that a network like the one shown in **Figure 3.1: Planar Graph** will not be 100% restorable under all double failure conditions, due to the nodes representing Zurich and Madrid only having a nodal degree of two. Effectively this means that, if the links between Zurich and Paris and Zurich and Lyon break, Zurich will be isolated and no traffic could be routed there. The nodal degree is a constraint that can only be overcome by network topology modifications.

The assumption is made that a network topology is given and optimisation is done based on the given network.

3.3 CRITERIA FOR MEASURING RESILIENCE MECHANISMS

Different mechanisms have different strengths and weaknesses and can be measured according to the following criteria:

1. The percentage of traffic that can be restored. This can be offset by the priority of the traffic.

2. The time taken to restore the network or recovery time. This impacts on the types of traffic that can be restored.
3. The amount of backup capacity needed in the scheme to be able to recover a specific traffic situation. Increasing the capacity will also increase the cost of the network. This inherently impacts on the bandwidth ability supplied.
4. The delay and fluctuation thereof on a restored route is a very definite consideration, whether the mechanism will be implemented or not.
5. The complexity of the restoration procedure and other requirements placed on the network and nodes are vital considerations.
6. Scalability of the mechanism ensures sufficient performance with increase in the network traffic volumes.
7. Stability of the recovery mechanisms by the most appropriate setting of timing parameters.

3.3.1 Survivability

Survivability is the measure of the ability of a network to continue to provide service in the event of a failure. This is inherently an attribute of the network design or technology implemented and considers whether failures occur and how often failures occur. It is also an aspect of network reliability that quantifies the performance of a network under failure conditions [29]. Different parameters in network survivability planning are depicted in **Figure 3.2: Network survivability planning.**

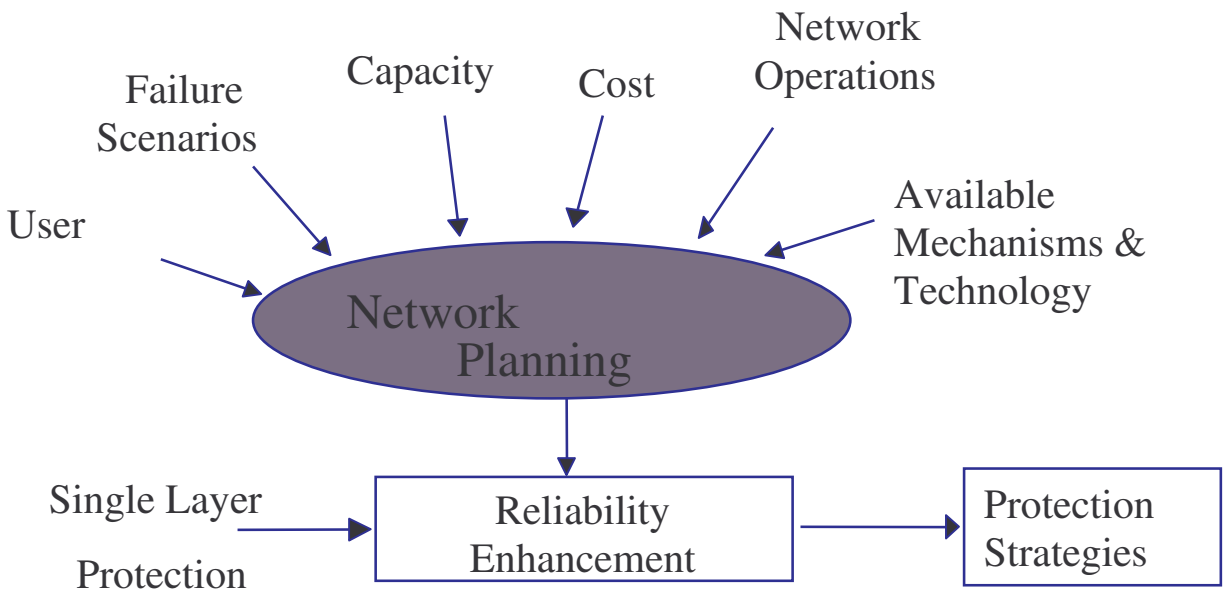


Figure 3.2: Network survivability planning

3.3.2 Restorability

Restorability is the most basic indication of survivability and is defined as the number of signal units that are restored after failure.

3.3.3 Reliability

According to Dixit and Ye [6], reliability is defined as:

> "…the probability of a device performing its purpose adequately for the period of time intended under the operating conditions intended."

The mean time to failure (MTTF) is a measure of reliability and is the time to the next failure following completion of repair. The mean time to repair (MTTR) is the time needed to recover from the failure. The mean time between failures (MTBF) includes both MTTF and MTTR and is effectively the time taken to restore the connection after failure and the subsequent time until the next failure occurs.

3.3.4 When can 100% restorability be achieved?

Availability is the measure of what the probability is of finding the system in working state when it is to be used [30]. The frequency of failures is of no relevance, but the speed of recovery in order not to notice downtime is critical. Availability is computed as follows [31]:

$$A = \left(\frac{MTBF}{MTBF + MTTR} \right)$$

Availability of 99.999% translates to off-service time of 5.256 minutes per year [8].

3.3.5 Quality of Resilience (QoR)

QoR is an insurance against failure scenarios or abnormal situations. It can therefore not be classified as part of QoS, but are combined with QoS to introduce better service offerings to the client. This additional focus area was brought in to incorporate the resilience considerations in network design.

3.3.6 Restorability vs. availability

If the network restorability design is for 100% restorability to all n-failure scenarios, "(n+1) failure" scenarios will result in unavailability. Practically, networks are 100% restorable if n = 0 (no failure scenario). Addition of redundancy is necessary to achieve n = 1, 2, etc. (full restorability against any single failures, dual failures, etc.) and gives a massive boost in *availability*.

Survivability and restorability are used as measures of the restoration process. The amount of backup capacity needed to ensure optimal restoration will also be commented on.

CHAPTER 4: EXPERIMENTAL METHODOLOGY AND APPROACH

4.1 INTRODUCTION

In this dissertation the wording experimental methodology and experimentation are used to include simulation and modelling.

Shared backup path protection (SBPP) with stub release was chosen for implementation and experimentation for the following reasons:

- The popularity of path protection is continuing to increase.
- Shared backup provides efficient use of network capacity.
- Less complexity than true path protection, which can be used to ensure that time constraints is met.
- No loopbacks are created in path protection, unlike link/span protection.
- A path-restorable network inherently provides a response to node-failures and multiple span failures within the same path. The whole path will be restored, irrespective of whether a single link or multiple links have failed on the same path.
- Path restoration also copes more gracefully with the multiple logical span failures arising from nodal "bypass" situations. **Figure 4.1: Span and Path restoration with multiple logical span failures** explains that, for path restoration, the same set of end-node connection pair failures arise in both logical and physical networks.

As mentioned in the section on assumptions, dual link-failures will be considered. Dual-link failures have been evaluated in the literature. Some interesting approaches were suggested in [32], [33] and [34], along with some others. In this study, dual-link failure recovery under specific network limitations, without knowledge of the specific second link failure, is investigated and a recovery algorithm implementation designed to provide fast and effective recovery.

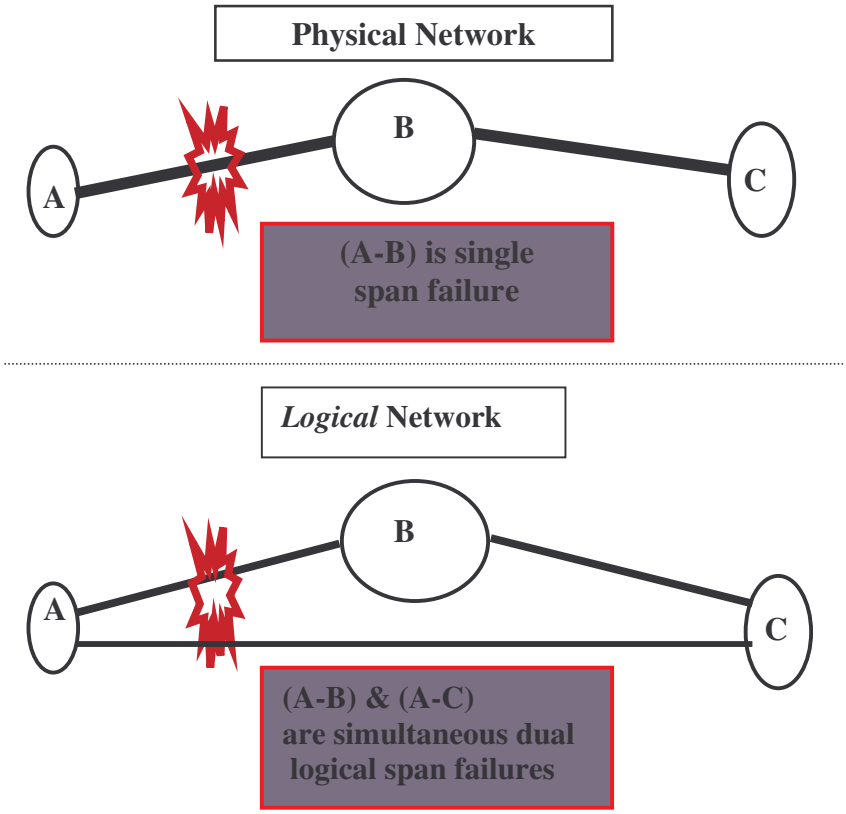


Figure 4.1: Span and Path restoration with multiple logical span failures

A single, fully disjoint backup path is established with each working path in a network. This network with primary and backup paths is simulated with the assumption that this is a test network and that the network topology and traffic modelling will be supplied in a practical scenario.

In effect, a 1:N APS distributed path arrangement is established. This simplifies the real time operation, since the response is independent of where the failure occurs on the corresponding working path. The releasing of surviving working capacity on the failed path after switching the path over is the only consideration (stub release), and is implemented to allow maximum reuse of the recoverable links. Different double-failure scenarios are simulated. A prioritised list of all components needed for establishing the simulation and the activities involved are given below and discussed subsequently:

1. Build traffic and network model for a test network and simplified PAN-European network.
2. Simulate networks without any restoration algorithm and capacity.
3. Simulate networks using shared backup path protection, using restoration algorithm and shortest path algorithm (Nicholson) for a first link failure.
4. Simulate networks using shared backup path protection, using restoration algorithm and shortest path algorithm (Nicholson) for a second link failure.
5. Comparison of outputs of 2, 3 and 4 using blocking probability and availability parameters.

Paths are computed in the network with **path length < ¾ * n,**
where n is the number of nodes in the network and ensures that no loopbacks occur in the path computations [12].

The sharebility of backup capacity is defined as the number of connections that share a backup link, and a value of two was chosen for this parameter. If this value is increased, the backup efficiency increases, but during failures more connections become unavailable or unprotected. This is also explained in section 4.4.2, when the simulation parameters are discussed.

4.2 NETWORK TOPOLOGY AND TRAFFIC MODEL

A simple fully-meshed network is used to test simulation functionality before the simulation is used for experimentation on more complex networks. The network has four nodes and five links and all nodes have a nodal degree of three. The network is given in **Figure 4.2: Simulation test network.**

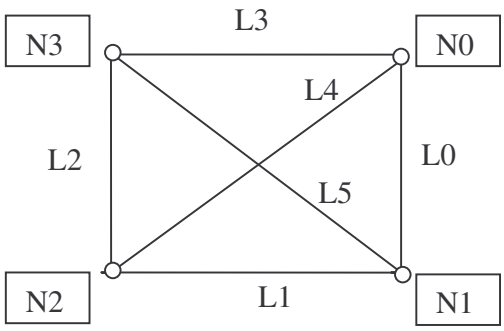


Figure 4.2: Simulation test network

The network topology that will be used in experimenting on research results is a simplified PAN-European network, designed as a joint effort of the IST project LION and COST action, which is a triangular network with high average nodal degree [35]. The total network and the portion used in the simulation are given in **Figure 4.3: PAN-European network and simulation network**. The impact of implemented solutions will be compared for service reliability and availability.

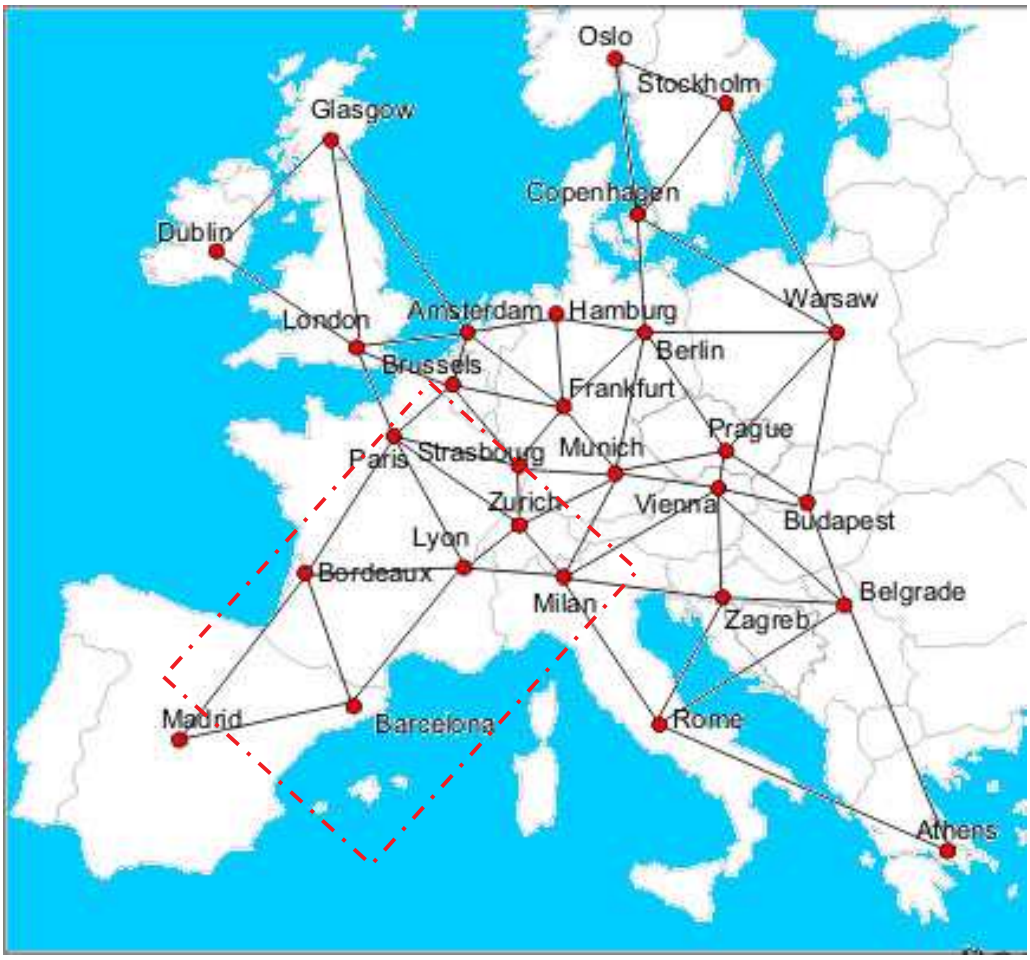


Figure 4.3: PAN-European network and simulation network as per Ghent University's INTEC Broadband Communication Networks (IBCN) Group drawing [35]

The network is presented as an incidence matrix that contains the distances and cost values of links between the nodes.

According to Gent University [35], the total traffic between city i and city j can be determined as a function of a constant K, the population P, the number of non-production business employees E, the number of Internet hosts H of the city region and the distance D between the cities as can be seen in **Table 4.1: European Traffic** model.

Table 4.1: European Traffic model

Voice Traffic	$K_v * P_i * P_j / D_{ij}^2$
Transaction Data Traffic	$K_t * E_i * E_j / D_{ij}$
IP Traffic	$K_i * H_i * H_j$

A uniform distribution of traffic connections was also used as a separate model for simulation experimentation purposes. A different network model was used for the PAN-European network, which gives more realistic traffic data. This model and the parameters used are discussed next.

The traffic estimations for the reference year 2002 as documented by Gent University [35], the values for the traffic constants over time and the estimation of the traffic growth were used to calculate the current and future traffic matrices for voice, transaction data and Internet traffic for the PAN-European network. A constant growth rate of 150% per annum over the time period 2002-2008 was used for IP traffic. For the voice traffic, a constant growth rate of 10% per annum has been estimated, while for the transaction data traffic a constant growth rate of 34% was used. **Table 4.2: Traffic models for Uniform (A) and model traffic data (B)**, shows typical network traffic data. Distance information was also utilised as a component of the link weights and is given in **Table 4.3: Distances between nodes in the network (km)**.

Link and node information is necessary in the simulation and therefore two matrices are used in the simulation, the first to represent node connections and the second to represent link. Refer to Section 4.3.1 for more details.

Table 4.2: Traffic models for Uniform (A) and model traffic (B) for 2005 (Gbps)

A:	Barcelona	Bordeaux	Lyon	Madrid	Paris	Zurich
Barcelona	0	12582.89	2193.051	13109.8	26846.65	10160.34
Bordeaux	25909.83	0	29349.74	21504.53	11702.79	30362.06
Lyon	11889.8	1821.837	0	14285.05	16726.24	10688.53
Madrid	23622.96	30789.4	672.529	0	7181.656	22990.28
Paris	27163.83	32996.01	33405.55	6542.361	0	7443.428
Zurich	13881.49	7035.231	7065.462	2398.68	32917.88	0
B:	**Barcelona**	**Bordeaux**	**Lyon**	**Madrid**	**Paris**	**Zurich**
Barcelona	0	12334.04	10768.49	14157.27	7925.792	6956.798
Bordeaux	12334.04	0	9949.177	10390.92	8905.156	5761.702
Lyon	10768.49	9949.177	0	7529.838	10738.64	9045.05
Madrid	14157.27	10390.92	7529.838	0	6961.069	6075.803
Paris	7925.792	8905.156	10738.64	6961.069	0	7134.772
Zurich	6956.798	5761.702	9045.05	6075.803	7134.772	0

Table 4.3: Distances between nodes in the network (km)

	Barcelona	Bordeaux	Lyon	Madrid	Paris	Zurich
Barcelona	0	670	796	760	1251	1257
Bordeaux	670	0	650	834	747	1135
Lyon	796	650	0	1367	594	507
Madrid	760	834	1367	0	1500	1561
Paris	1251	747	594	1500	0	735
Zurich	1257	1135	507	1561	735	0

4.3 NETWORK SIMULATION

A simulation program was developed in order to experiment on the performance of SBPP under specific network topological conditions. The input variables, parameters and working of the simulation are discussed below.

4.3.1 Input Variables:

The simulation receives the following data:

- The network node topology in the form of a node matrix containing the weights/connectivity between nodes.
- The network link topology in the form of a node matrix containing the link numbers per node pair.
- The number of distinct paths in the network.
- The number of connections per path.
- The connections matrix supplying the current primary and protection paths for the network.

4.4 RESTORATION SIMULATION

Before a failure scenario the network is considered stable and protected, since all connections established have a protection path assigned to the connection. If, however, a failure occurs, either working connections, protection connections or a combination of both are affected, making the network unavailable and unprotected to additional failures. If a connection has lost its primary connection, it is currently unavailable until the connection is switched over to its protection path (if available) and is then only unprotected, but not lost. If a protection path is lost, the working path of that connection is also unprotected.

4.4.1 Link Matrix

A link matrix is utilised to represent the link between working and protection paths. It is an incidence matrix representing all links in the network. The number of wavelengths reserved on link e as backup wavelengths for connections traversing e' is given as the value $L_e^{e'}$, where **L** is

the link matrix. This is an uncomplicated data structure that is also very efficient to represent the relationship between working and protection paths.

4.4.2 Algorithm

Parameters:

- e* is the failed link.
- N_e^{e*} is the number of connections whose primary path utilised the failed link, e* and backup connection uses link e.
- N_e is the number of connections whose backup connection uses link e.
- c_e is the available wavelengths on e after e* has failed. This is computed by subtracting the number of wavelengths lost during failure by the number of reserved wavelengths that was necessary before failure, taking into account the sharebility factor.
- f(e) is the number of unused wavelengths.
- S is the sharebility between protection connections.

  The sharebility values, as well as the total number of wavelengths available on each link, are constants that are fixed before network simulation.

Algorithm after each failure occurs:

1. Switch all affected primary paths to backup paths.
2. Update all variables, the connection matrix, the link matrix, etc.
3. Compute the number of available wavelengths.
4. Perform "stub release" on all wavelengths not affected by the failure and which can be reused.
5. Reprovision a new backup for each unprotected connection. This includes new backups for the affected primary paths and the affected backup paths.

   The algorithm used for the weights is a modified version of the algorithm used in [27] for each link (Assume that the primary path traverses links e1,e2,…,em)

$$\text{Weight}(e) = \begin{cases} \infty & \text{if e is on primary path of connection or e = failed link,} \\ 0 & \text{if } L_e^{e1} < c_e, \ldots, L_e^{em} < c_e, \text{ and } [(N_e + 1)/ c_e] <= S, \\ w & \text{if } f(e)>0, \ w \text{ is the distance weight of each connection,} \\ \infty & \text{otherwise} \end{cases} \quad (1)$$

$e \quad , \forall e \in E$

Apply the shortest path algorithm discussed in Section 4.4.3, using the applied link costs.

6. Update all variables and the connection and link matrix.
7. Compute availability and restorability.

4.4.3 Shortest Path Algorithm

The calculation to discover the shortest route between two points has many variations and algorithms. Finding the shortest route sounds simple enough in concept, but much time can be wasted if inefficient methods are used. These types of algorithms are integral in a number of network computations and very important in network optimisation design.

It is of cardinal importance to choose a well-tested algorithm that produces optimal results and minimises computation time. Nicholson's algorithm [36] has been around for many years. The procedure is to examine all the routes from a starting point **s** and from the termination point **t** simultaneously, and to extend the route that has covered the shortest distance. This is continued until the shortest route from **s** has a node that concur with a node on the shortest route from **t**. The route is then checked to make sure that it is indeed the shortest route.

The reason for choosing this algorithm instead of the popular Dijkstra algorithm is the possible superior performance. According to [A2], Nicholson's shortest path algorithm [36] is about 60 times faster than Dijkstra's. The algorithm and additional notes are given below.

Parameters

n is the number of junction points.

d_{ij} is the distance between connection points i and j.

s is the starting point.

t is the terminating point.

S(i) is the current minimum distance from s to i.

P(i) is the point preceding i in the current optimal route from s to i.

Q(i) is the point preceding i in the current optimal route from i to t.

x is the current least distance from s.

y is the current least distance from t.

Initialisation values

$$\left.\begin{aligned} S(i) &= d_{si} \\ T(i) &= d_{it} \\ P(i) &= s \\ Q(i) &= t \end{aligned}\right\} \text{ for all } i \qquad (2)$$

Algorithm

The flow diagram is given in **Figure 4.4: Flow diagram of Nicholson's Shortest Path Algorithm**.

Note:

This algorithm is typically implemented having a fixed starting and end point. In the reprovisioning approach, any node can be the starting and termination nodes, since this is determined by the failure scenario. This necessitated that additional control had to be built in to make sure loopbacks do not occur.

An example is given for the simulation test network in **Figure 4.2: Simulation test network**, to demonstrate the procedure. First the matrix representing weights and distances is constructed, in which MAX = 99 is used to represent non-connected nodes. The initial values are given for S, P, T and Q. The changes to these values are given over the number of iterations necessary to find an

optimal route. The shortest distance from node to node is therefore **4** units and the route is computed as follows:

P(1),1 ,Q(1)

0, 1, 3

The working example can be seen in **Table 4.4: Working example of Nicholson's Shortest Path algorithm.**

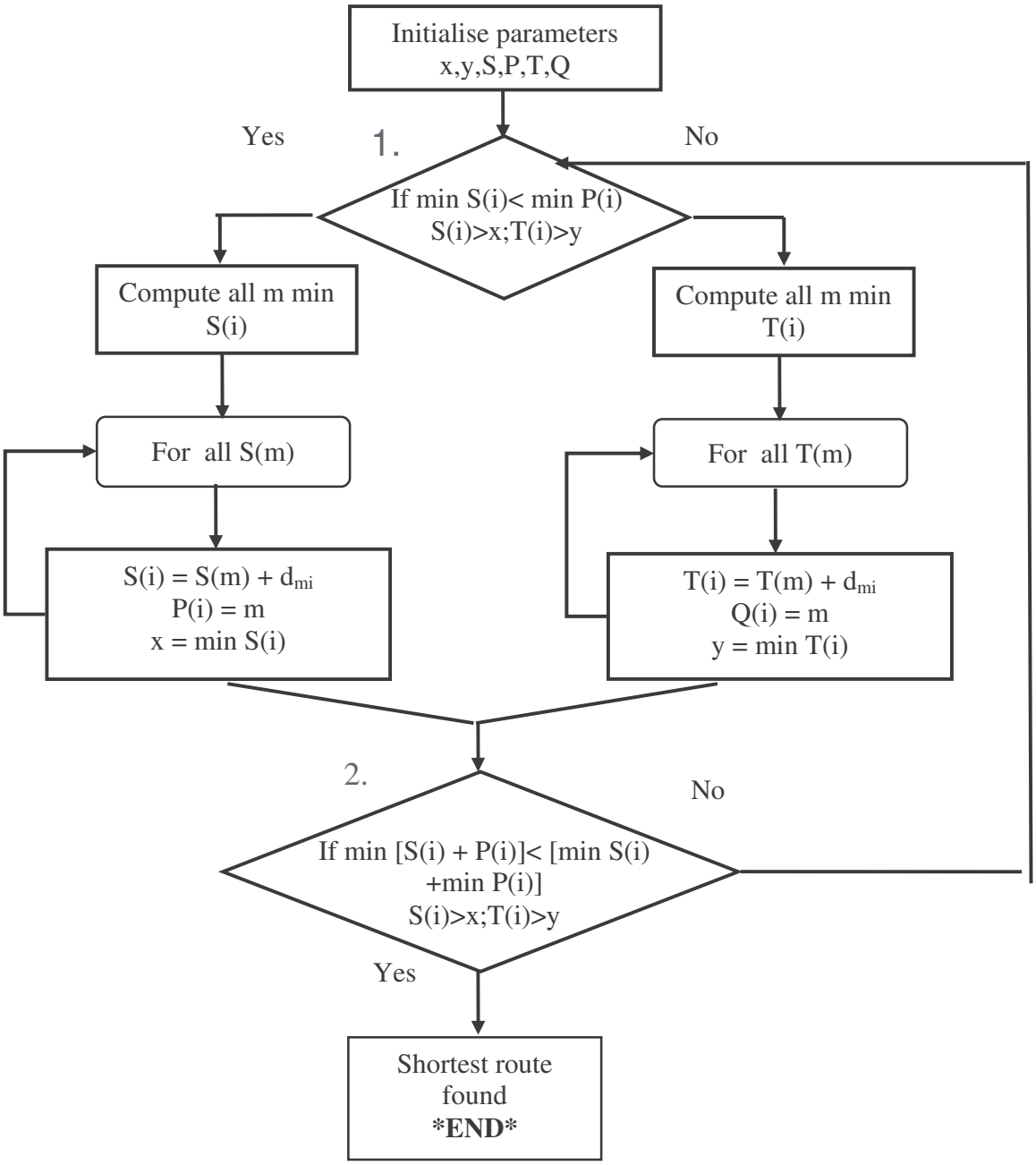
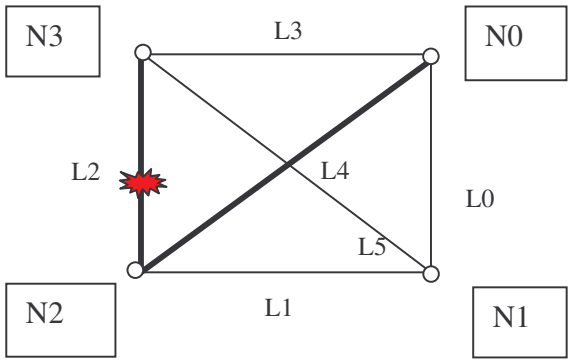


Figure 4.4: Flow diagram of Nicholson's Shortest Path Algorithm

Table 4.4: Working example of Nicholson's Shortest Path algorithm



Start node 3

End node 0

Resulting weight matrix

	N0	**N1**	**N2**	**N3**
N0	99	2	1	99
N1	2	99	2	2
N2	1	2	99	99
N3	99	2	99	99

Initial

S(i)	99	2	1	99
P(i)	0	0	0	0
T(i)	99	2	99	99
Q(i)	3	3	3	3

1st iteration

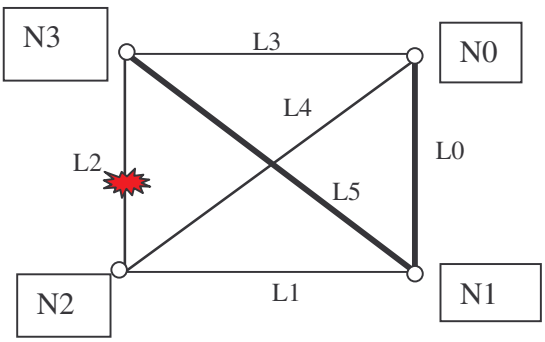
S(i)	99	2	1	4
P(i)	0	0	0	1
T(i)	99	2	99	99
Q(i)	3	3	3	3

PATH (nodes)

0, 1, 3, 99,

PATH (links)

0 5



4.5 DESIGN TOOLS AND METHODOLOGY

The project consists mainly of software-designed modules on a personal computer (PC) functional unit that provides the interfaces between the software modules and performs the calculations. This integrates the network simulation module and the optimisation of resilience algorithm modules in a control plane.

4.6 FUNCTIONAL ANALYSIS

The system has the main functional units given below:

- **FU 1: Network Architecture.** The network architecture simulation will form a large part of the project and will incorporate the network topology and parameters for fibre types, etc.
- **FU 2**: Reprovisioning module.
- **FU 3**: Shortest path computation unit.

The functional components of the system are given in **Figure 4.5: Functional block diagram of the system**.

4.7 SYSTEM SPECIFICATIONS

The specifications of the system are the most important part of the objectives. The specifications that were adhered to are given next. This is done for each functional unit.

FU 1: The network architecture simulation should contain all the nodes of the simplified PAN-European network and the traffic modelling as discussed in Section 4.2. Weights according to the distances between nodes can also be implemented.
FU 2: This module should switch protection paths to primary paths, perform “stub release” and reprovision new routes accurately.

FU 3: The shortest path computation should achieve the shortest possible path without any loops within a 10^{th} of a second.

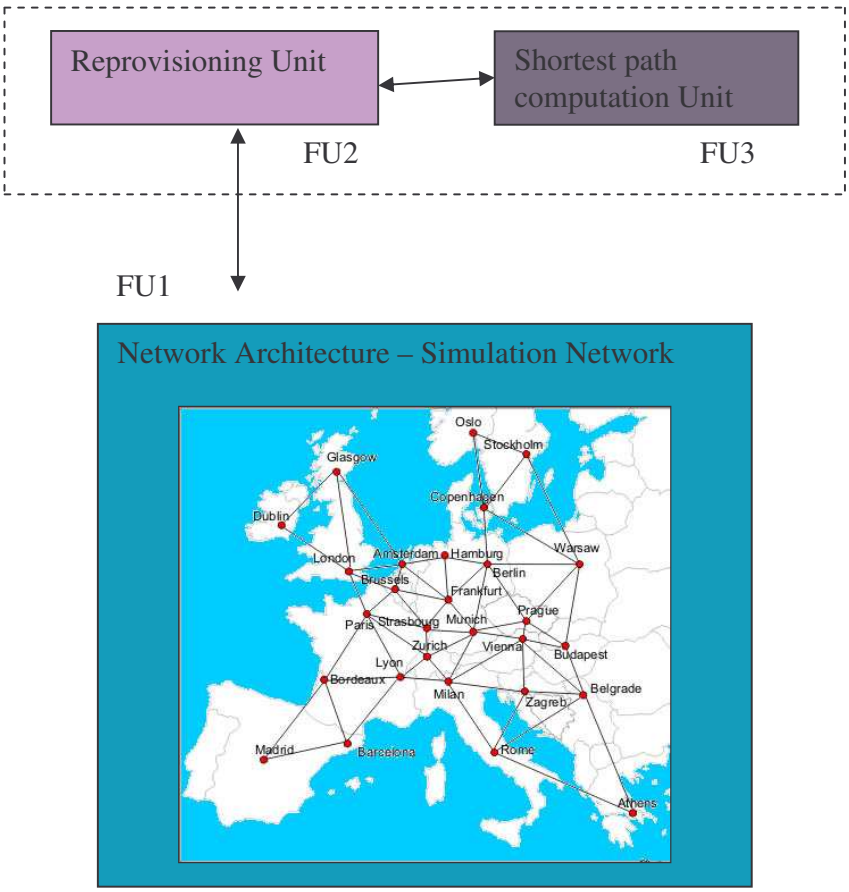


Figure 4.5: Functional block diagram of the system

4.9 SYSTEM FLOW DIAGRAM

The system flow diagram is given in **Figure 4.6: Overall system flow diagram**.

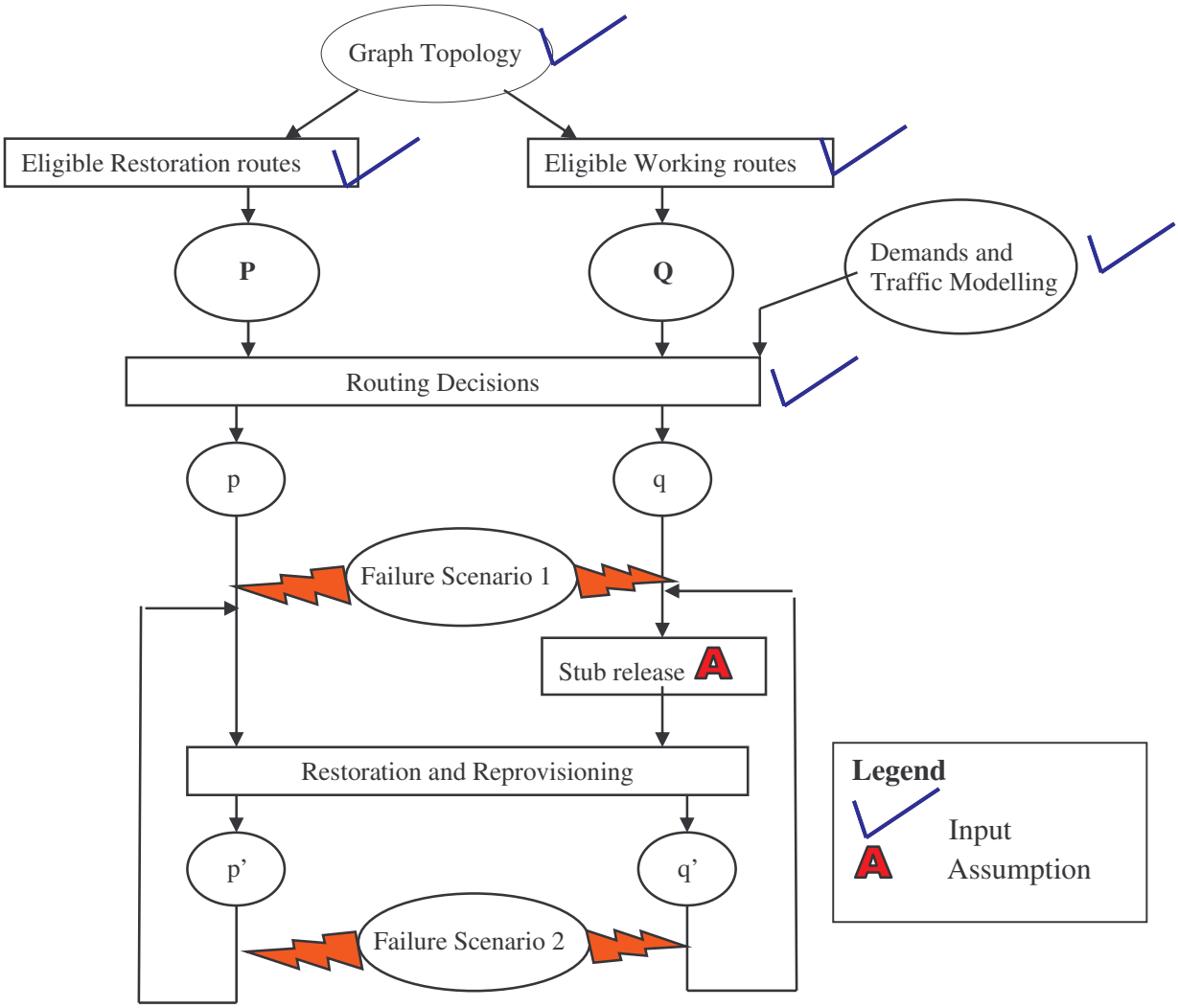


Figure 4.6: Overall system flow diagram

CHAPTER 5: SIMULATION TEST RESULTS

5.1 INTRODUCTION

In this section the experimentation is done and simulations are produced for the simulation test network to illustrate the functionality of the system. Also in this section, experimentation results for the simplified PAN-European network are presented to analyse practical output. It remains to compare the test network and practical network with practical traffic data. As a precursor to SBPP, static path protection was implemented and some results are also shown.

5.2 STATIC PATH PROTECTION

The working of static path protection is discussed here for illustration purposes only. **Table 5.1: Path table for SPP** shows an example of a network link table containing the working path (w1) and all possible pre-allocated protection paths (pr1, pr2, pr3, pr4 and pr5). These protection paths are used in order as network failures occur. The following assumptions were made in this experiment:

- The wavelength availability was already checked at connection establishment.
- Unlimited wavelength availability.
- **Table 5.1: Path table for SPP** contains working path and span disjoint paths to working path; protection paths are therefore not necessarily span disjoint – limiting routing options.

The advantage of this method is that it is simple and fast.

The disadvantage of this method is that it is static. The routes are added to a routes table by the network administrator, which might not present optimal routes. Another disadvantage is that protection is unassured, or a best-effort approach.

A graphical representation of this method is given in:

Figure 5.1: SPP before first failure;

Figure 5.2: SPP after first failure; and

Figure 5.3: SPP after second failure.

Notes:

- Links become more congested after each failure.
- According to the link table, the brown link no longer has a backup path after the second failure.

Table 5.1: Path table for SPP

PATHS	NODES	w1	pr1	pr2	pr3	pr4	pr5	Demand	Capacity
1	N1-N2	1	2,3	2,5,4	2,6,7,4			2	24
2	N1-N3	2	1,3	1,4,5	1,4,7,6			6	24
3	N1-N4	1,4	2,5	2,6,7	2,6,8,9			7	24
4	N1-N5	2,6	1,4,7	1,3,5,7	1,4,9,8			3	24
5	N1-N6	1,4,9	2,6,8	2,5,7,8				1	24
6	N2-N3	3	1,2	4,5	4,7,6	4,9,8,6		2	24
7	N2-N4	4	3,5	1,2,5	3,6,7	1,2,6,7	3,6,8,9	0	24
8	N2-N5	3,6	4,7	4,9,8				10	24
9	N2-N6	4,9	3,6,8	3,5,7,8	1,2,6,8			2	24
10	N3-N4	5	3,4	6,7	4,1,2	9,8,6		3	24
11	N3-N5	6	5,7	5,9,8	7,4,3	2,1,4,7	3,4,9,8	0	24
12	N3-N6	6,8	5,9	3,4,9	2,1,4,9			12	24
13	N4-N5	7	9,8	5,6	4,3,6	4,1,2,6		3	24
14	N4-N6	9	7,8	5,6,8	4,3,6,8			6	24
15	N5-N6	8	7,9	6,5,9	6,3,4,9			12	24

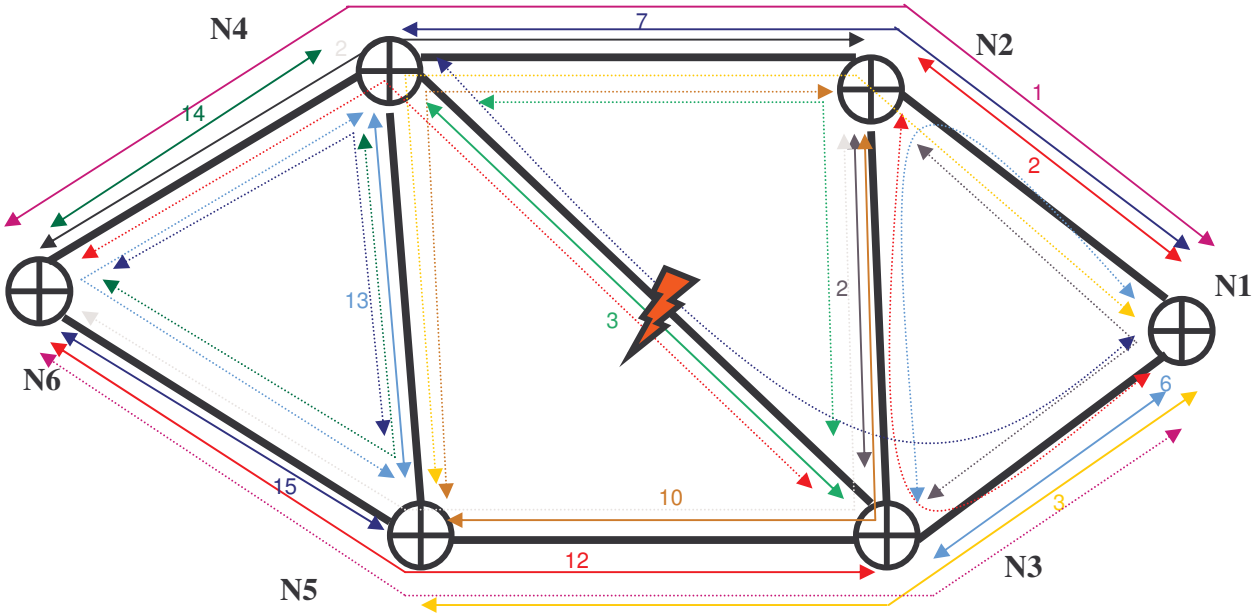


Figure 5.1: SPP before first failure

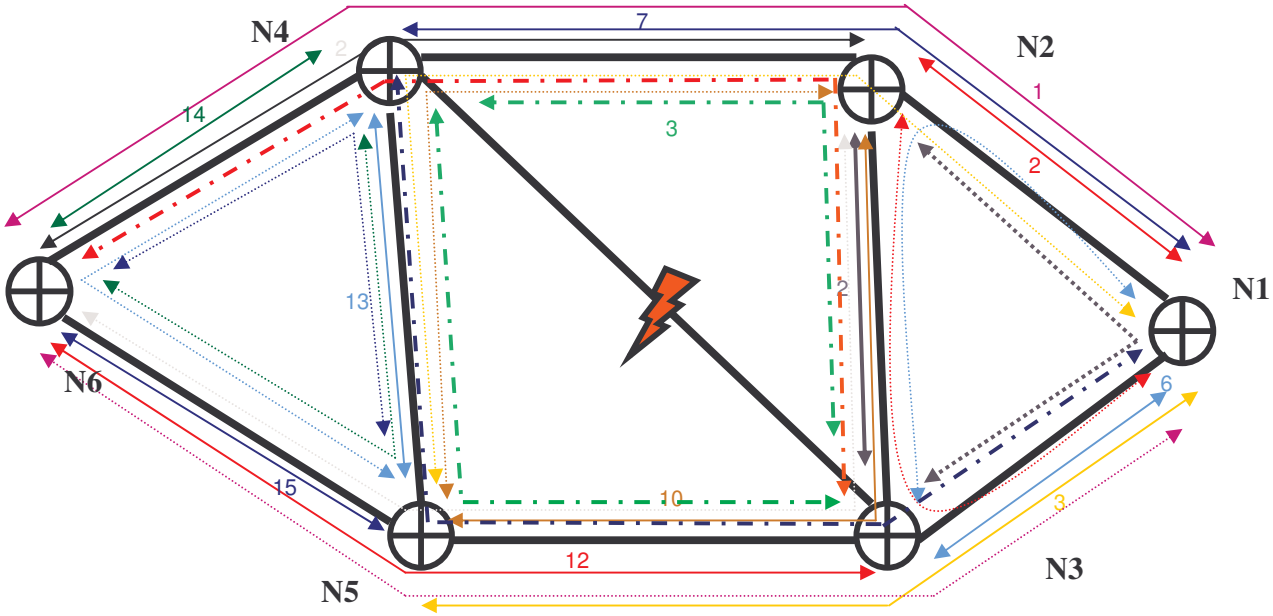


Figure 5.2: SPP after first failure

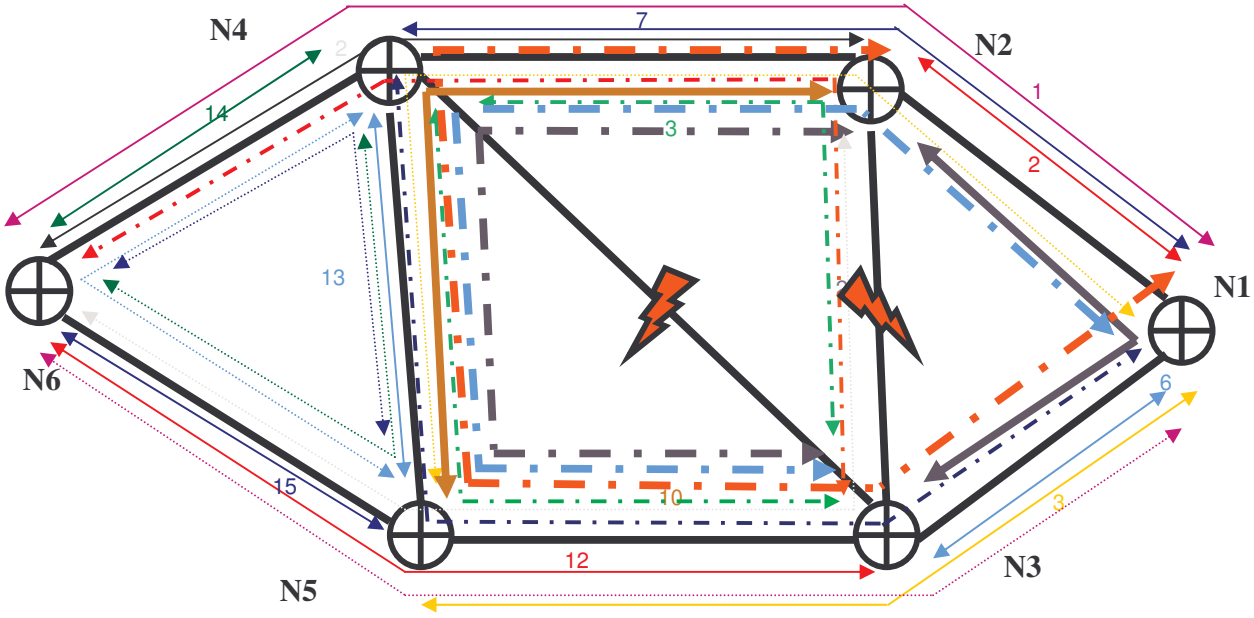


Figure 5.3: SPP after second failure

5.3 SHARED BACKUP PATH PROTECTION

5.3.1 Test network simulation – parameters, assumptions and results

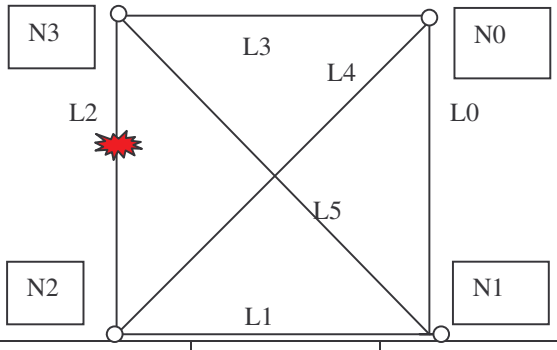
The simple network discussed in Section 4.2 is used to test simulation functionality.

- Each link has 16 wavelengths available for connections.
- A conservative network load of 6 connections per link was chosen for the test.
- A protection wavelength sharing factor of 2 was chosen.
- This brings the total network load containing primary and protection connections to 75%.
- A bidirectional link failure is simulated and the unavailability (1 – availability) and unprotectability (1 – protectability) computed. An example of a failure is given in **Figure 5.4: Example of first failure** and **Table 5.2: Example of first failure**. The results are shown in graphical format in **Figure 5.5: Graph of results for first failure on test network.**
- New paths are then reprovisioned for all affected connections. The connection unavailability and unprotectability are again computed after reprovisioning. These results are given in **Figure 5.6: Example of first reprovisioning, Table 5.3: Example of first reprovisioning** and **Figure 5.7: Graph of results for first reprovisioning on test network**.
- A second bidirectional link failure is then simulated and unavailability and unprotectability computed before reprovisioning. These results are given in **Table 5.4: Example of second failure, Figure 5.8: Example of second failure** and **Figure 5.9: Graph of results on second failure on test network.**
- Reprovisioning is done again and availability and protectability computed. These results are given in **Figure 5.10: Example of second reprovisioning, Figure 5.11: Graph of results for second reprovisioning on test network** and **Table 5.5: Example of second reprovisioning**.
- These values are also compared to the unavailability and unprotectability after the first failure. These results are given in **Figure 5.12: Before and after comparison for SBPP.**

This was done for all possible failure combinations to ascertain whether the simulation does indeed produce accurate results.

5.3.2 Simulation results

5.3.2.1 Network after failure of link 2 (first failure) and before reprovisioning



Paths affected

Failure Link	2
Total Capacity/Link	16

PATHS	NODES	Working Path Links	Protection Path Links	Demand (working capacity) (frequency)	Backup (backup capacity) (f)
0	N0-N1	0	3	6	6
0	N0-N1	99	5	6	6
0	N0-N1	99	99	6	6
0	N0-N1	99	99	6	6
1	N0-N2	4	0	6	6
1	N0-N2	99	1	6	6
1	N0-N2	99	99	6	6
2	N0-N3	3	4	6	6
2	N0-N3	99	2	6	6
2	N0-N3	99	99	6	6
3	N1-N2	1	0	6	6
3	N1-N2	99	4	6	6
3	N1-N2	99	99	6	6
3	N1-N2	99	99	6	6
4	N1-N3	5	1	6	6
4	N1-N3	99	2	6	6
4	N1-N3	99	99	6	6
4	N1-N3	99	99	6	6
5	N2-N3	2	1	6	6
5	N2-N3	99	5	6	6
5	N2-N3	99	99	6	6

Figure 5.4: Example of first failure

Table 5.2: Example of first failure

	Connections usage:				
SPAN	Working paths	Protection paths	Working frequencies	Protection frequencies	Total
0	1	2	6	12	12
1	1	3	6	18	15
2	1	2	6	12	12
3	1	1	6	6	9
4	1	2	6	12	12
5	1	2	6	12	12
Percentage usage:			37.50%	37.50%	75.00%
Unavailability:			6/36	16.67%	
Unprotectability			18/36	50.00%	

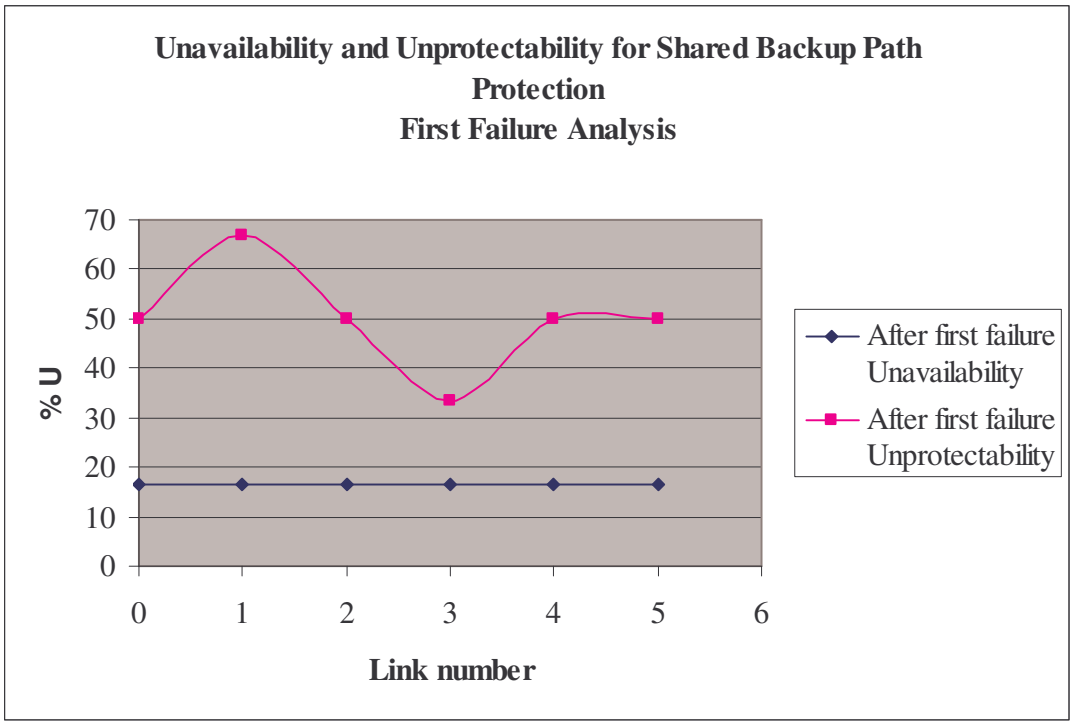
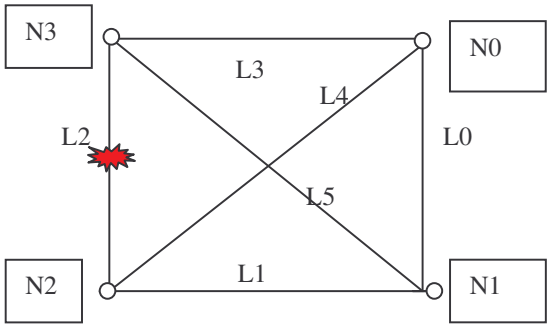


Figure 5.5: Graph of results for first failure on test network

5.3.2.2 Network after failure of link 2 (first failure) and after reprovisioning



Paths affected

Failure Link	2
Total Capacity/Link	16

PATHS	NODES	Working Path Links	Protection Path Links	Demand (working capacity) (f)	Backup (backup capacity) (f)	Total Capacity (f)
0	N0-N1	0	3	6	6	16
0	N0-N1	99	5	6	6	16
0	N0-N1	99	99	6	6	16
0	N0-N1	99	99	6	6	16
1	N0-N2	4	0	6	6	16
1	N0-N2	99	1	6	6	16
1	N0-N2	99	99	6	6	16
1	N0-N2	99	99	6	6	16
2	N0-N3	3	0	6	2	16
2	N0-N3	99	5	6	2	16
2	N0-N3	99	99	6	2	16
3	N1-N2	1	0	6	6	16
3	N1-N2	99	4	6	6	16
3	N1-N2	99	99	6	6	16
3	N1-N2	99	99	6	6	16
4	N1-N3	5	0	6	6	16
4	N1-N3	99	3	6	6	16
4	N1-N3	99	99	6	6	16
4	N1-N3	99	99	6	6	16
5	N2-N3	1	4	6	6	16
5	N2-N3	5	3	6	6	16
5	N2-N3	99	99	6	6	16

Figure 5.6: Example of first reprovisioning

Table 5.3: Example of first reprovisioning

	Connections usage				
SPAN	Working paths	Protection paths	Working frequencies	Protection frequencies	Total
0	1	4	6	20	16
1	2	1	12	6	15
2	0	0	0	0	0
3	1	3	6	18	15
4	1	2	6	12	12
5	2	2	12	8	16
Percentage usage:			43.75%	33.33%	77.08%
Unavailability			0/36	0.00%	
Unprotectability:			4/36	11.11%	

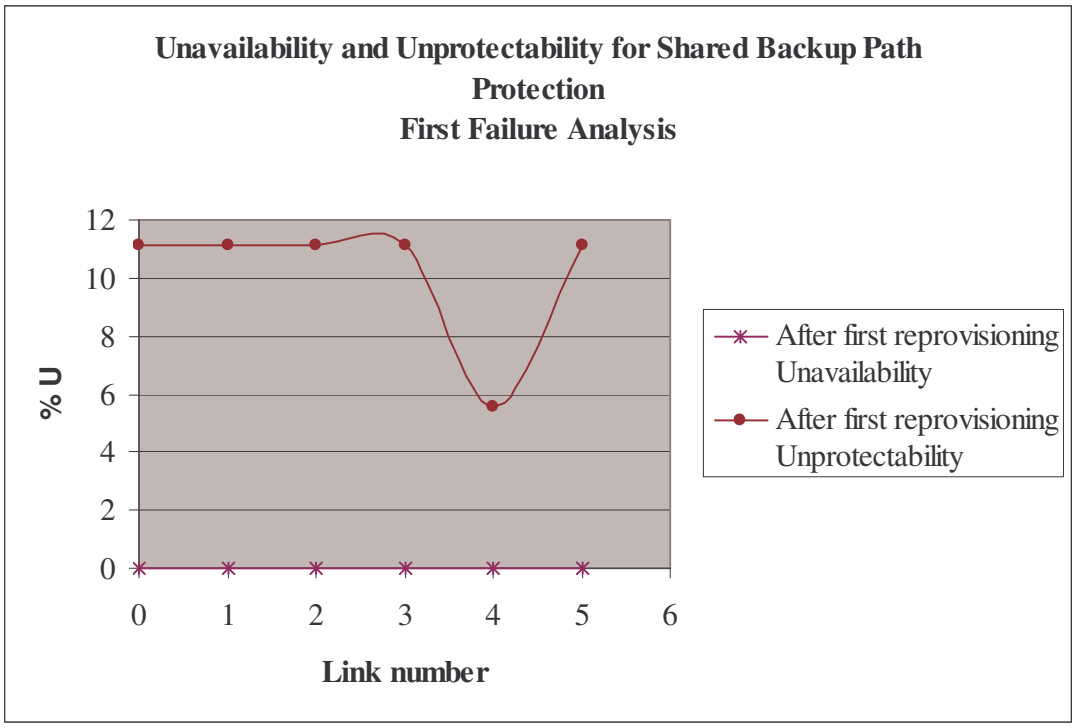
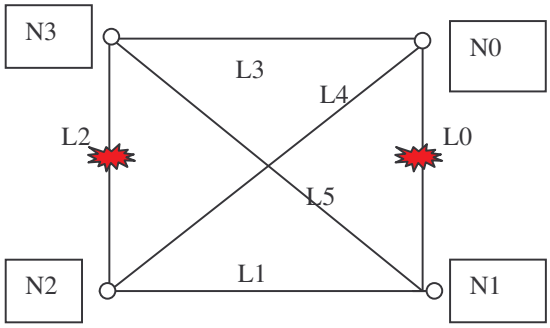


Figure 5.7: Graph of results for first reprovisioning on test network

5.3.2.3 Network after failure of link 0 (second failure) and before reprovisioning



Paths affected

Failure Link	0
Total Capacity/Link	16

PATHS	NODES	Working Path Links	Protection Path Links	Demand (working capacity) (f)	Backup (backup capacity)(f)	Total Capacity (f)
0	N0-N1	0	3	6	6	16
0	N0-N1	99	5	6	6	16
0	N0-N1	99	99	6	6	16
0	N0-N1	99	99	6	6	16
1	N0-N2	4	0	6	6	16
1	N0-N2	99	1	6	6	16
1	N0-N2	99	99	6	6	16
1	N0-N2	99	99	6	6	16
2	N0-N3	3	0	6	2	16
2	N0-N3	99	5	6	2	16
2	N0-N3	99	99	6	2	16
3	N1-N2	1	0	6	6	16
3	N1-N2	99	4	6	6	16
3	N1-N2	99	99	6	6	16
3	N1-N2	99	99	6	6	16
4	N1-N3	5	0	6	6	16
4	N1-N3	99	3	6	6	16
4	N1-N3	99	99	6	6	16
4	N1-N3	99	99	6	6	16
5	N2-N3	1	4	6	6	16
5	N2-N3	5	3	6	6	16
5	N2-N3	99	99	6	6	16

Figure 5.8: Example of second failure

Table 5.4: Example of second failure

	Connections usage				
SPAN	Working paths	Protection paths	Working frequencies	Protection frequencies	Total
0	1	4	6	20	16
1	2	1	12	6	15
2	0	0	0	0	0
3	1	3	6	18	15
4	1	2	6	12	12
5	2	2	12	8	16
Percentage usage:			43.75%	33.33%	77.08%
Unavailability:			6/36	16.67%	
Unprotectability:			30/36	83.33%	

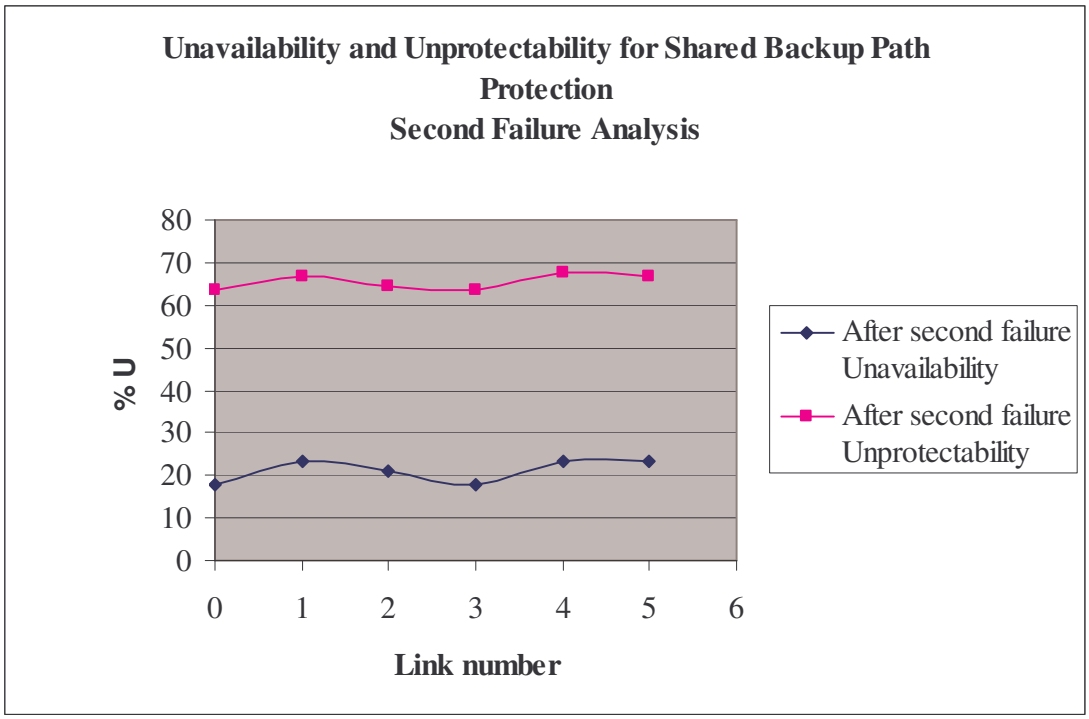
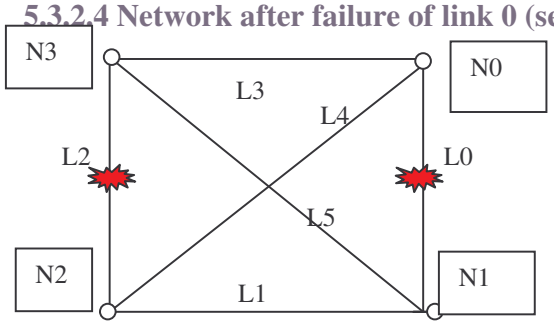


Figure 5.9: Graph of results on second failure on test network

5.3.2.4 Network after failure of link 0 (second failure) and after reprovisioning



Paths affected

Failure Link	0
Total Capacity/Link	16

PATHS	NODES	Working Path Links	Protection Path Links	Demand (working capacity) (f)	Backup (backup capacity) (f)	Total Capacity (f)
0	N0-N1	3	1	4	4	16
0	N0-N1	5	4	4	4	16
0	N0-N1	99	99	4	4	16
0	N0-N1	99	99	4	4	16
0	N0-N1	1	99	2	6	16
0	N0-N1	4	99	2	6	16
0	N0-N1	99	99	2	6	16
0	N0-N1	99	99	2	6	16
1	N0-N2	4	99	6	6	16
1	N0-N2	99	99	6	6	16
1	N0-N2	99	99	6	6	16
1	N0-N2	99	99	6	6	16
2	N0-N3	3	99	6	6	16
2	N0-N3	99	99	6	6	16
2	N0-N3	99	99	6	6	16
3	N1-N2	1	99	6	6	16
3	N1-N2	99	99	6	6	16
3	N1-N2	99	99	6	6	16
4	N1-N3	5	99	6	6	16
4	N1-N3	99	99	6	6	16
4	N1-N3	99	99	6	6	16
4	N1-N3	99	99	6	6	16
5	N2-N3	1	4	6	6	16
5	N2-N3	5	3	6	6	16
5	N2-N3	99	99	6	6	16

Figure 5.10: Example of second reprovisioning

Table 5.5: Example of second reprovisioning

	Connections usage				
SPAN	Working paths	Protection paths	Working frequencies	Protection frequencies	Total
0	0	0	0	0	0
1	3	1	14	4	16
2	0	0	0	0	0
3	2	1	10	6	13
4	2	2	8	10	13
5	3	0	12	0	12
Percentage usage:			45.83%	10.42%	56.25%
Unavailability:			0/36	0.00%	
Unprotectability:			26/36	72.22%	

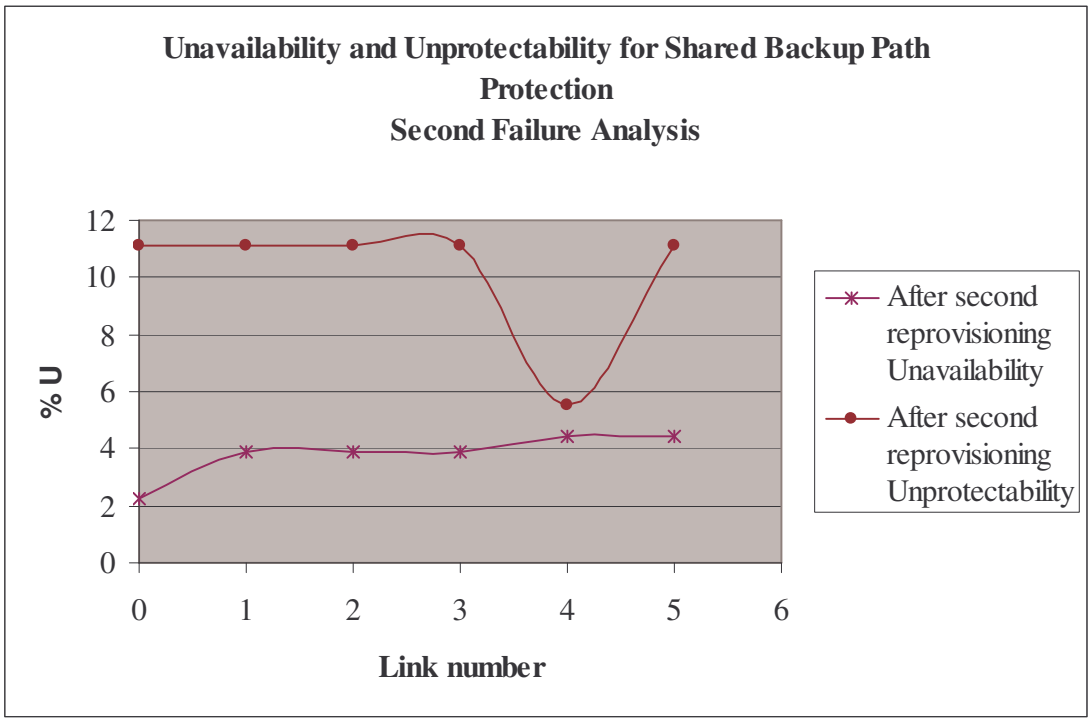


Figure 5.11: Graph of results for second reprovisioning on test network

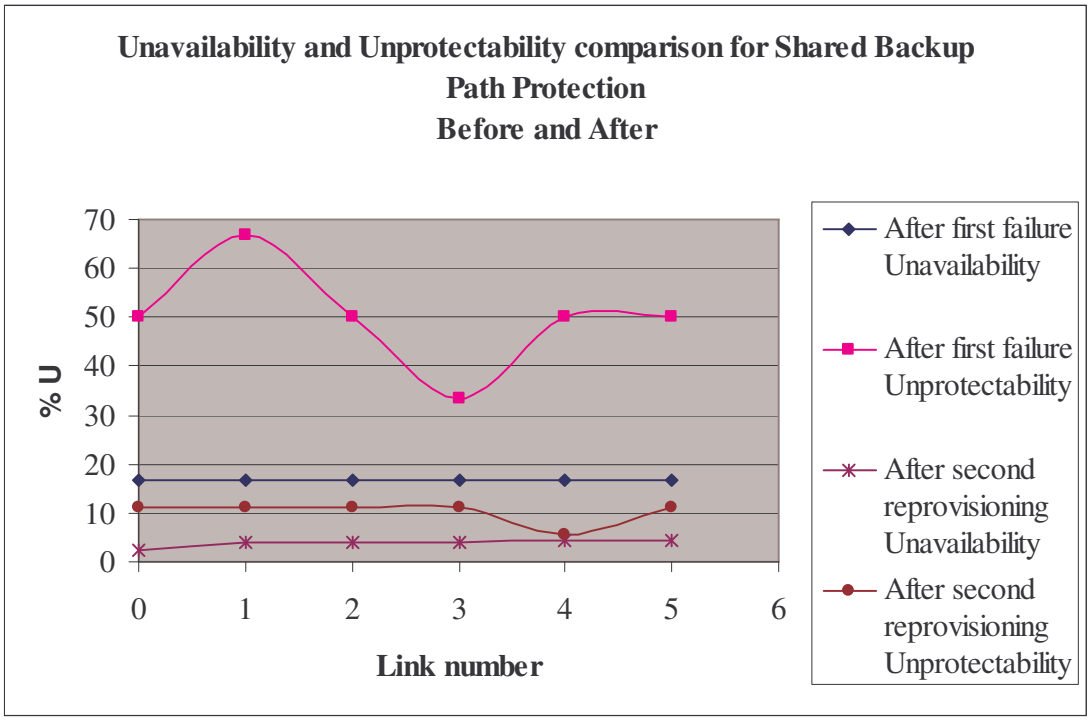


Figure 5.12: Before and after comparison for SBPP on test network

5.3.3 PAN-European network simulation – parameters, assumptions and results

The simulation tool was developed and data extracted for the PAN-European network. The following assumptions were made in this experiment:

- The wavelength availability was already checked at connection establishment.
- Limited wavelength availability.

It can be seen from the graphs that follow that the results obtained are much less encouraging than the results achieved in Section 5.3.2.

5.3.3.1 Network after first failure, before and after reprovisioning

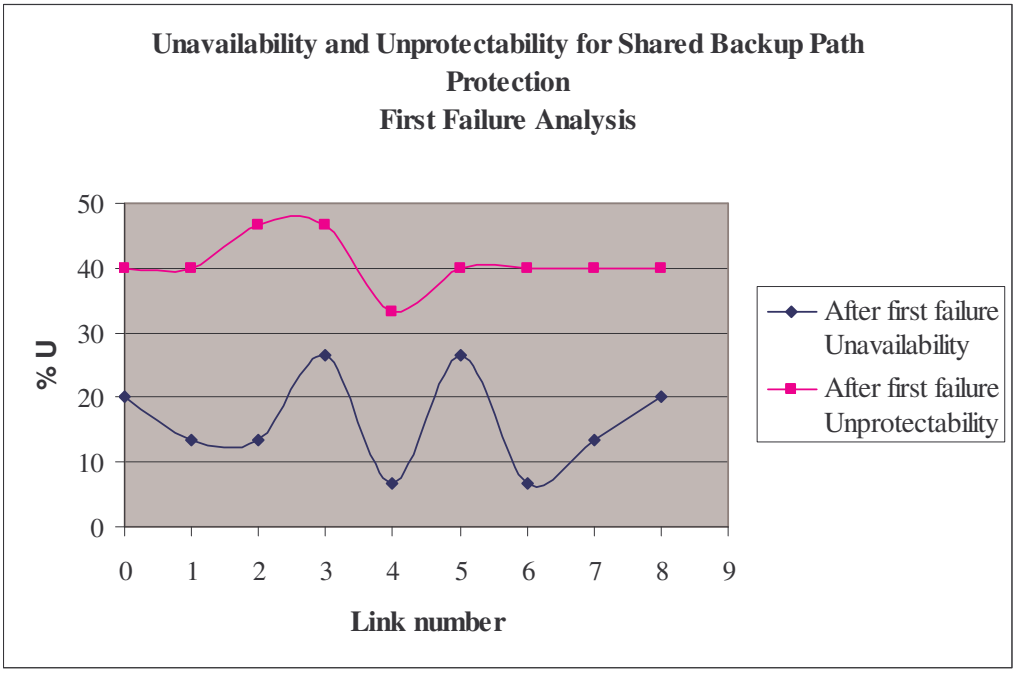


Figure 5.13: SBPP Analysis for a practical backbone network – first failure before reprovisioning

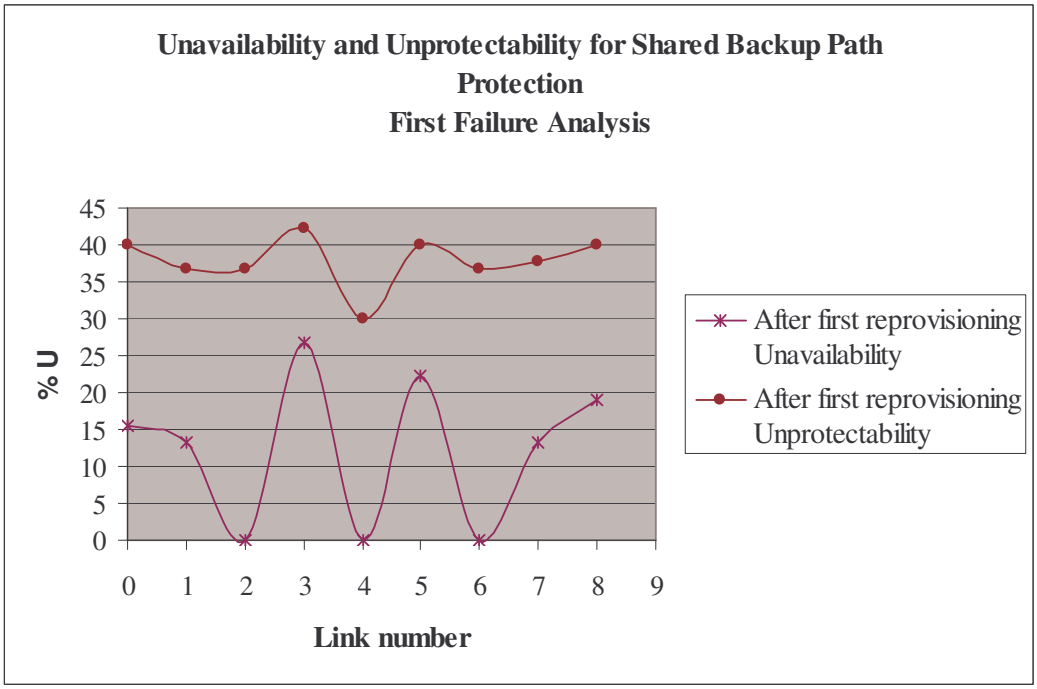


Figure 5.14: SBPP Analysis for a practical backbone network – first failure after reprovisioning

5.3.3.2 Network after second failure, before and after reprovisioning

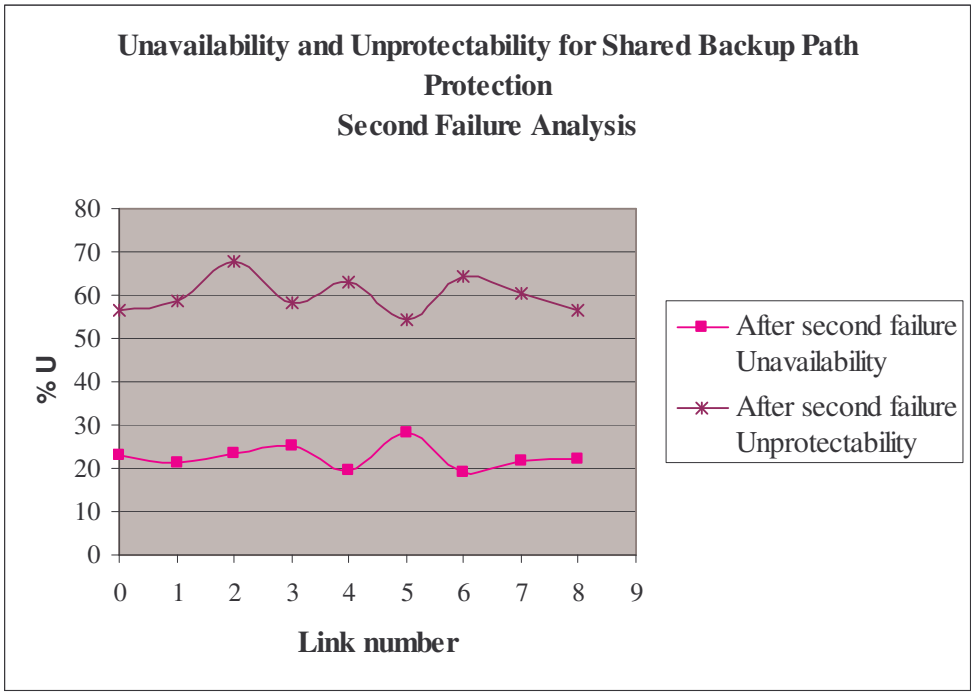


Figure 5.15: BPP Analysis for a practical backbone network – second failure before reprovisioning

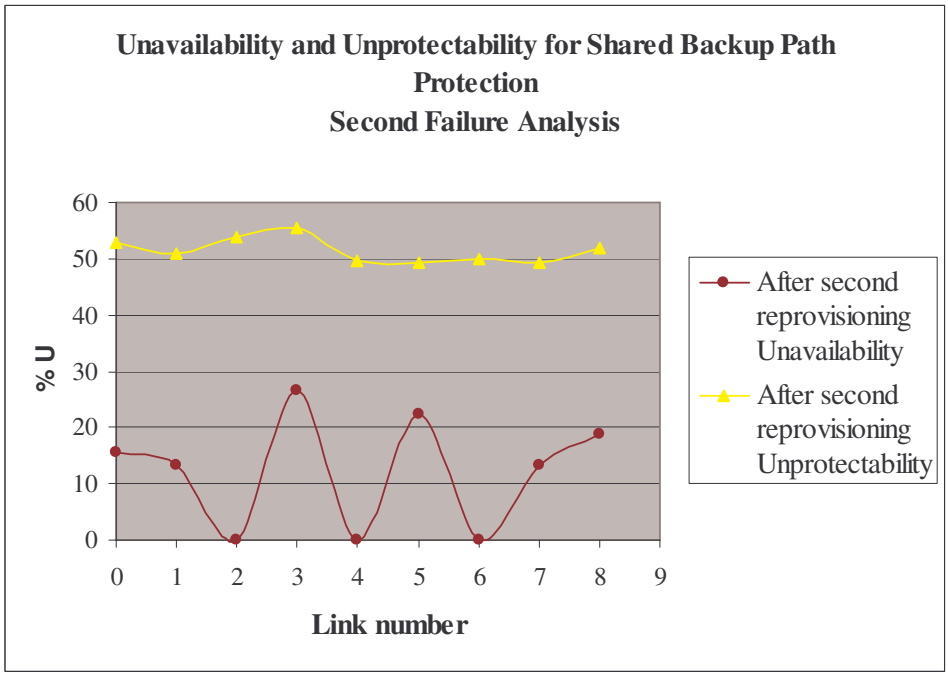


Figure 5.16: BPP Analysis for a practical backbone network – second failure after reprovisioning

5.3.4 Explanation and analysis of results

Figures 5.4, 5.6, 5.8 and 5.10 depict the primary and protection links used at the different network states. The percentage unavailability and unprotectability (%U), as well as network usage for the specific example, is given in each of the tables that follow the figures. Figures 5.5, 5.7, 5.9 and 5.11 give the results as a percentage of unavailability and unprotectability (%U) averaged over all possible failure scenarios for the simulation test network, and Figures 5.13 - 5.16 give the same results for the PAN-European network.

The unavailability of the simulation test network before the first failure is a smooth line with an average of 16%. The unavailability of the PAN-European network is much more volatile, but with the same average of 16%. The unprotectability of the two networks is much higher than the unavailability, with an average of around 50%.

The unavailability of the simulation test network after the first failure and subsequent recovery is reduced to 0% due to the protection paths available, which is link disjoint to the working paths. The unavailability of the PAN-European network is again much more volatile, and has values of 0% for certain links, but with the same average of 12%. The unprotectability of the two networks is much higher than the unavailability, with an average of 10% and 37% respectively.

The unavailability of the simulation test network after the second failure is again relatively smooth with an average of 20%, which is higher than after the first failure. This can be expected, due to the fact that the network becomes more congested and more connections are therefore affected with the second failure. The unavailability of the PAN-European network is again much more volatile, but with a comparable average of 22%. The unprotectability of the two networks is again much higher than the unavailability, for the same reason as explained above, with an average of 65% and 60% respectively.

The unavailability of the simulation test network after the second failure recovery is reduced to 4%, due to the protection paths available, which is link disjoint to the working paths. The unavailability of the PAN-European network is again much more volatile, and has values of 0%

for certain links, but with the same average of 22%. This graph follows the same pattern as the first failure graph. The average unprotectability of the two networks is 20% and 51% respectively.

Figure 5.12: Before and after comparison for SBPP shows that the protection success is tremendous. The comparison of the availability after the first failure and after the second reprovisioning shows a 12 % improvement in availability and 40 % improvement in unprotectability, and that after two failures!

The results for the simplified PAN-European network are less promising. The average of the availability after the first failure and after the second reprovisioning is 16 % before and 22% afterwards. The unprotectability has average values of 50% and 51% before the first failure recovery and after the second failure recovery, which is still extremely positive, since very little availability was compromised after two failures.

If compared with SPP, this method is much more flexible, producing fast and effective results.

CHAPTER 6: CONCLUSION

6.1 INTRODUCTION

For continually-growing optical networks, network management and protection functions need to be addressed as an integral part of improvement of the availability of networking components, subsystems and the network as a whole.

In this dissertation, only a part of control and management of optical networks was covered. Besides network survivability (fault management), connection management and automatic topology discovery (configuration management) are key points for deployment of optical WDM and DWDM networks [37].

The conclusion regarding the results and advantages and disadvantages of the shared backup path protection implementation is given next.

6.2 SUMMARY

As can be seen from the experimental results given in Chapter 5, shared backup path protection provides enhanced network availability under failure scenarios. An additional advantage of shared backup path protection is the quick response, due to the fact that a backup route is pre-computed. A new backup for affected connections can be computed in the background when processing power is available, after restoration.

The network restorability is offset by the additional cost involved in ensuring suitable spare capacity for protection paths. A suitable balance needs to be achieved between the amount of shared backup capacity and the ability to restore networks, since the more the connections share a backup route, the less chance of all connections being restored after failure.

Spare capacity occupies a substantial part of the network, since backup paths are likely to be longer and occupy more wavelengths than the working path. This results in reserving more capacity on the network.

Dual-link failures can easily be protected by the use of this simulation. Due to the fact that the precise link that has failed doesn't need to be found, the algorithm is less complicated than span protection.

Table 6.1: Multiple failure performance analysis

	Single Failure Restorability	**Double failure Restorability**
Shortest Backup Path Protection 1	1.0000	0.8804
Shortest Backup Path Protection 2	1.0000	0.9620
Shortest Backup Path Protection 3	0.87777	0.77083

Table 6.1: Multiple failure performance analysis, shows the comparison of SBPP for different network topology scenarios.

Row one contains results obtained in [38], [39] and [40].

Row two contains the results of the simulation test network. As expected, in this highly-meshed network with flat capacity (same capacities on every link) and conservative capacity usage, the shortest backup path plan for link restoration works very well, better than line one under double failure scenarios.

Row three contains the results obtained from the simplified PAN-European network. The average network restorability remains high (around 80%), even for dual-link failure scenarios. The network topology has a very big impact on the restorability of the network. **Figure 6.1: Example of network topology effect on network protection** depicts one scenario.

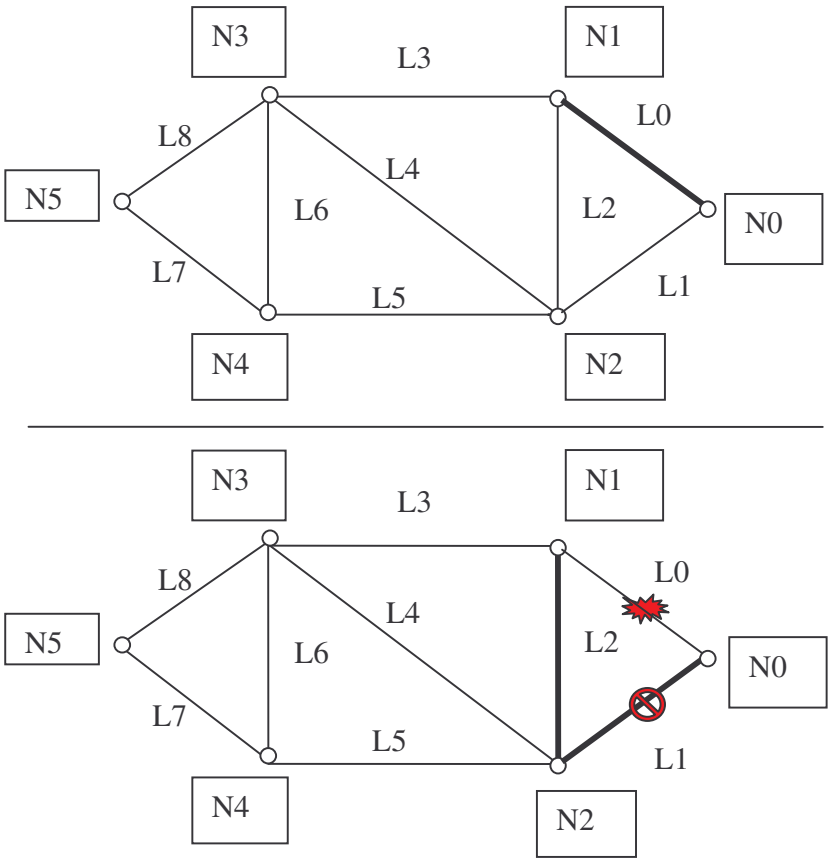


Figure 6.1: Example of network topology effect on network protection

A connection is set up between node 0 (N0) and node 1 (N1). If link 0 (L0) fails, this connection is switched over to the protection path L1 – L2. Both links from N0 are now unavailable. Unless a new link is established, no more protection advantages can be gained by this node. The nodal degree is therefore a very big factor that impacts on protection design.

6.3 ASSESSMENT OF STUDY

As set out at the start of the project, network resilience algorithms and methods were investigated. Traffic models were established to assist in modelling network usage. It was proven that optimisation and resilience can add valuable improvement in optical network performance. It was further concluded that, for specific network limitations such as in backbone networks, certain methods can enhance service delivery and add economic benefit.

The implementation of SBPP is therefore a necessity in highly-meshed networks with high availability needs, but doesn't necessarily provide the best solution for sparsely-connected networks. This is ideal for high priority or (national) security traffic. The additional cost involved in the implementation is in the order of 30%, with effective sharebility parameters for backup protection and needs to be considered carefully. This figure is computed by dividing a path increase of 100% by a sharebility factor of 3.

6.3 RECOMMENDATION FOR FUTURE WORK

In this study the assumption was made that a network topology was fixed and optimisation was done based on the fixed network. An alternative approach would be to use statistical data for traffic modelling and design an optimal network topology using path restoration as a given. Pure path restoration is also a field that can be explored.

REFERENCES

[1] ITU-T Recommendation G.8080/Y.1304: Architecture for the automatically switched optical network (ASON), pp. 1-48, November 2001.

[2] G. Keiser, *Optical Fibre Communications*, Third Edition, McGraw-Hill, New York, USA, 2000, pp. 71-78.

[3] M. Mcdard, S. S. Lumetta, Y. -C. Tseng, "Capacity-Efficient Restoration for Optical Networks", *Optical Fiber Communication Conference, 2000*, Volume 3, 7-10 March 2000, pp.207-209.

[4] D. D. Harms, M. Kraetzl, C. J. Colbourn, and J. S. Devitt, "*Network Reliability",* Boca Raton, FL: CRC Press, USA, 1995, pp. 22-23.

[5] D.A. Schupke, A. Autenrieth, and T. Fischer, "Survivability of Multiple Fiber Duct Failures", *in Proceedings of International Workshop on Design of Reliable Communication Networks,* Volume 1, 2001, pp. 1-5.

[6] S. Dixit and Y. Ye, "Streamlining the Internet-Fiber Connection", *IEEE SPECTRUM,* Volume 38, Issue 4, April 2001, pp. 52-57.

[7] R. Ramaswami, K. N. Sivarajan, *Optical Networks - A Practical Perspective*, Second Edition, Academic Press, San Diego, USA, 2002, pp. 537-587.

[8] P. Demeester, "Recovery in Multilayer, Multidomain & Multiservice Core Networks", *in International Workshop on Design of Reliable Communication Networks*, Volume 5, pp.13-17, 16-19 October 2005.

[9] J. P. Ryan, "WDM: North American deployment trends", *IEEE Communications Magazine*, Volume 36, pp. 40-44, February 1998.

[10] E. Lowe, "Current European WDM deployment trends", *IEEE Communications Magazine*, Volume 36, pp. 46-50, February 1998.

[11] B. Wen, N. M. Bhide, R. K. Shenai, and K. M. Sivalingam, "Optical Wavelength Division Multiplexing (WDM) Network Simulator (*OWns*): Architecture and Performance Studies", *School of Electrical Engineering & Computer Science Washington State University*, Pullman, WA 99164, pp. 1-30, 1999.

[12] R. Bhandari, "*Survivable Networks: Algorithms for Diverse Routing*," First edition, Kluwer Academic Publishers, USA, pp. 106-112, 1999.

[13] W. D. Grover, *Mesh-Based Survivable Networks*, First Edition, Prentice Hall, New Jersey, USA, 2004, pp. 59-60, 109, 115, 118-200.

[14] S. Ruepp, L. Dittmann, and L. Ellegård, "Simulation and Comparison of Path Restoration Techniques in SDH Mesh Networks", *in Proceedings of International Workshop on Design of Reliable Communication Networks*, Volume 5, pp. 1-7, 16-19 October 2005.

[15] G. Ellinas, "Fault Restoration in Optical Networks with Arbitrary Mesh Topologies," at http://m.ctzcolumbia.edu/-georg'os/APS.html. Last accessed on 2 April 2005.

[16] J. Doucette and W.D. Grover, "Comparison of Mesh Protection and Restoration Schemes and the Dependency on Graph Connectivity," *in Proceedings of International Workshop on Design of Reliable Communication Networks,* Volume 1, 2001, pp. 30-35.

[17] S. S. Lumetta and M. M'edard, "Towards deeper understanding of link restoration algorithms for mesh networks", *in Proceedings Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, *IEEE INFOCOM 2001,* Volume 1, 2001, pp.367-375.

[18] B. van Caenegem, N. Wauters, and P. Demeester," Spare capacity assignment for different restoration strategies in mesh survivable networks", *IEEE International Conference on Communications, 1997. ICC 97 Montreal, 'Towards the Knowledge Millennium',* Volume 1, 8-12 June 1997, pp. 288-292.

[19] G. Ellinas, E. Bouillet, R. Ramamurthy, J.-F. Labourdette, S. Chaudhuri, K. Bala "Routing and restoration architectures in mesh optical networks," *Optical Networks Magazine*, Volume 4, Issue 1, January/February 2003, pp. 42-48.

[20] J. Vasseur, M. Picavet, P. Demeester, *Network Recovery*, First Edition, Morgan Kaufmann Publishers, San Francisco, USA, pp. 20-55, 2004.

[21] T. E. Stern, K. Bala, *Multiwavelength Optical Networks - A Layered Approach*, First Edition, Prentice Hall, New Jersey, USA, 2002, pp. 12-56.

[22] R. Ramaswami and A. Segall, "Distributed network control for optical networks," *IEEE/ACM Transactions on Networking*, Volume 5, No. 6, pp. 936-943, December 1997.

[23] S. S. Lumetta and M. Medard, "Towards a deeper understanding of link restoration algorithms for mesh networks," *in Proceedings Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, Volume 1, pp. 367-375, 22-26 Apr. 2001.

[24] R. Ramamurthy, A. Akyamac, J. F. Labourdette, and S. Chaudhuri, "Preemptive reprovisioning in mesh optical networks," *in Proceedings Optical Fibre Communications Conference, 2003. OFC 2003*, Volume 1, pp. 785-787, March 2003.

[25] J. Strand, AT&T Labs, "Converging Protection and Restoration Strategies of the IP and Optical Layers to Support the Survival of IP Services", *MPLS Next Generation Networking Summit*, pp. 1-5, January 2001.

[26] W. Grover, J. Doucette, M. Clouqueur, D. Leung, D. Stamatelakis, "New Options and Insights for Survivable Transport Networks", *IEEE Communications Magazine,* Volume 40, Issue 1, pp.34-41, January 2002.

[27] J. Zhang, K. Zhu, and B. Mukherjee, "A Comprehensive Study on Backup Reprovisioning to Remedy the Effect of Multiple-Link Failures in WDM Mesh Networks", *in Proceedings of IEEE international Conference on Communications*, Volume 3, pp.1654-1658, 20-24 June 2004.

[28] D. Schupke and R. Prinz, "Performance of path protection and rerouting for WDM networks subject to dual failures," *in Proceedings Optical Fibre Communications Conference, 2003. OFC 2003*, Volume 1, pp. 209-210, 23-28 March 2003.

[29] S. S. Lumetta, M. Medard, and Y. C. Tseng, "Capacity versus robustness: a trade-off for link restoration in mesh networks," *IEEE/OSA Journal of Lightwave Technology*, Volume 18, No. 12, pp. 1765-1775, December 2000.

[30] G. Weichenberg and W.D. Grover, "Availability analysis of span restorable mesh networks", *in Proceedings of Conference of Optical Society of America*, June 2003, pp. 12-18.

[31] M. Clouqueur and W. D. Grover, "Availability Analysis of Span-Restorable Mesh Networks", *IEEE Journal on Selected Areas in Communications*, Volume 20, No. 4, May 2002, pp.810-821.

[32] H. Komine, T. Chujo, T. Ogura, K. Miyazaki, and T. Soejima, "A distributed restoration algorithm for multiple-link and node failures of transport networks," *in Proceedings IEEE Global Telecommunications Conference, 1990, and Exhibition. 'Communications: Connecting the Future', GLOBECOM '90,* Volume 1, pp. 459-463, 2-5 Dec. 1990.

[33] *E. Ayanogly,* "A Fast Topology Update Algorithm for Restoration under Multiple Failures in Broadband Networks", *IEEE International Conference on Communications, 1993. ICC 93. Geneva,* Volume 3, 23-26 May 1993, pp. 1295-1299.

[34] M. Clouqueur and W. D. Grover, "Dual failure availability analysis of span-restorable mesh networks," *IEEE Journal on Selected Areas in Communications,* Volume 20, No. 4, May 2002, pp. 120-128.

[35] Ghent University's INTEC Broadband Communication Networks (IBCN) Group, "PAN-European Triangular Network", http://www.ibcn.intec.ugent.be/css_design/research/projects/IST_FP5/NRS. Last accessed on 5 July 2005.

[36] T.A.J. Nicholson, "Finding the shortest route between two points in a network", *The Computer Journal*, Volume 6, pp. 275-280, 1966.

[37] B. Ramamurthy, L. Shen, and E. Sawma, "Connection Management for Wavelength-routed Optical WDM Networks", *Magazine on Advances in Optical Networks*, Volume 1, 2002, pp. 1-3.

[38] S. S. Heydari and O. Yang, "Multiple Failure Analysis with Restoration Paths Matrix", *in Proceedings of Global Telecommunications Conference, IEEE GLOBECOM '04*, pp. 2098-2102, 29 November-3 December 2004.

[39] H. Choi, S. Subramaniam, and H.-A. Choi, "On double-link failure recovery in WDM optical networks," *in Proceedings Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, *IEEE INFOCOM 2002,* Volume 2, pp. 808-816, June 2002.

[40] S. Kim and S. Lumetta, "Evaluation of protection reconfiguration for multiple failures in WDM mesh networks," *in Proceedings Optical Fibre Communications Conference, 2003. OFC 2003*, Volume 1, pp. 210-211, 23-28 March 2003.

APPENDIX 1: ADDITIONAL READING MATERIAL

A1.1 DWDM

[A1] http://www.iec.org/online/tutorials/dwdm/. Last accessed on 3 October 2005.

A1.2 Shortest path algorithms

[A2] "Shortest Path Citations",
http://citeseer.ifi.unizh.ch/context/280502/0. Last accessed on 11 October 2005.
[A3] "Dijkstra",
www.ifors.ms.unimelb.edu.au/tutorial/dijkstra_new. Last accessed on 11 October 2005.
[A4] http://www-unix.mcs.anl.gov/dbpp/text/node1.html. Last accessed on 11 October 2005.
[A5] http://www.cs.sunysb.edu/~algorith/files/shortest-path.shtml. Last accessed on 11 October 2005.

A1.2 Survivability and Resilience

[A6] W. Tsong-Ho, "Emerging Technologies for Fibre Network Survivability", *IEEE Communications Magazine*, Volume 33, Issue 2, pp. 62-74, February 1995.
[A7] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *IEEE/OSA Journal of Lightwave Technology*, Volume 21, No. 4, pp. 870-883, April 2003.
[A8] B. Melian, J.A. Moreno, M. Laguna, "Survivability in WDM networks", *Simposio de Informática y Telecomunicaciones (SIT'02)*, pp.201-210, 2002.
[A9] http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/af5/report.html. Last accessed on June 2004.
[A10] "Comparison of Resilience Mechanisms for Dynamic Services in Intelligent Optical Networks", *in Proceedings of International Workshop on Design of Reliable Communication Networks*, Volume 3, pp. 106-113, October 2003.
[A11] M. Clouqueur and W. D. Grover, "Availability analysis of spanrestorable mesh networks," *IEEE Journal on Selected Areas in Communications*, Volume 20, No. 4, pp. 810-821, May 2002.

APPENDIX 2: EXPERIMENTAL DATA

Table A2.1: First failure analysis data for simplified PAN-European network

	Unavailability	Unprotectability			Unavailability	Unprotectability
0	20	40		0	15.555555	40
1	13.333333	40		1	13.333333	36.666668
2	13.333333	46.666668		2	0	36.666668
3	26.666666	46.666668		3	26.666666	42.222221
4	6.666667	33.333332		4	0	30
5	26.666666	40		5	22.222221	40
6	6.666667	40		6	0	36.666668
7	13.333333	40		7	13.333333	37.777779
8	20	40		8	18.888889	40
	16.29629611	**40.74074089**			**12.22222189**	**37.77777822**

Table A2.2: Second failure analysis data for simplified PAN-European network

Nodes				Nodes			
1st failure	2nd failure	Unavailability	Unprotectability	1st failure	2nd failure	Unavailability	Unprotectability
0	1	15.555555	22.222221	0	1	33.333332	24.444445
0	2	22.222221	56.666668	0	2	27.777779	51.111111
0	3	28.888889	66.666664	0	3	27.777779	51.111111
0	4	22.222221	65.555557	0	4	22.222221	51.111111
0	5	35.555557	60	0	5	37.777779	51.111111
0	6	22.222221	73.333336	0	6	21.111111	51.111111
0	7	28.888889	73.333336	0	7	24.444445	54.444443
0	8	28.888889	73.333336	0	8	24.444445	51.111111
1	0	13.333333	16.666666	1	0	33.333332	23.333334
1	2	23.333334	63.333332	1	2	26.666666	51.111111
1	3	26.666666	53.333332	1	3	35.555557	53.333332
1	4	20	66.666664	1	4	13.333333	47.777779
1	5	33.333332	63.333332	1	5	13.333333	43.333332
1	6	20	70	1	6	20	51.111111
1	7	26.666666	70	1	7	26.666666	50
1	8	26.666666	63.333332	1	8	28.888889	56.666668
2	0	13.333333	46.666668	2	0	20	66.666664
2	1	10	50	2	1	26.666666	64.444443
2	3	13.333333	53.333332	2	3	26.666666	66.666664

2	4	6.666667	66.666664	2	4	0	61.111111
2	5	20	56.666668	2	5	6.666667	54.444443
2	6	6.666667	70	2	6	6.666667	64.444443
2	7	13.333333	70	2	7	13.333333	64.444443
2	8	13.333333	63.333332	2	8	15.555555	67.777779
3	0	28.888889	62.222221	3	0	28.888889	44.444443
3	1	33.333332	60	3	1	32.222221	44.444443
3	2	33.333332	60	3	2	32.222221	44.444443
3	4	26.666666	53.333332	3	4	31.111111	37.777779
3	5	40	46.666668	3	5	42.222221	37.777779
3	6	33.333332	73.333336	3	6	26.666666	51.111111
3	7	40	73.333336	3	7	26.666666	51.111111
3	8	33.333332	73.333336	3	8	26.666666	51.111111
4	0	13.333333	56.666668	4	0	15.555555	63.333332
4	1	13.333333	63.333332	4	1	13.333333	61.111111
4	2	13.333333	60	4	2	0	60
4	3	13.333333	40	4	3	33.333332	60
4	5	16.666666	50	4	5	26.666666	60
4	6	6.666667	63.333332	4	6	0	56.666668
4	7	10	63.333332	4	7	13.333333	55.555557
4	8	20	66.666664	4	8	15.555555	66.666664
5	0	35.555557	60	5	0	34.444443	44.444443
5	1	28.888889	63.333332	5	1	25.555555	44.444443
5	2	28.888889	73.333336	5	2	6.666667	47.777779
5	3	35.555557	46.666668	5	3	43.333332	37.777779
5	4	28.888889	55.555557	5	4	30	37.777779
5	6	28.888889	55.555557	5	6	33.333332	37.777779
5	7	28.888889	60	5	7	28.888889	37.777779
5	8	28.888889	46.666668	5	8	35.555557	37.777779
6	0	20	72.222221	6	0	15.555555	68.888885
6	1	8.888889	67.777779	6	1	13.333333	63.333332
6	2	7.777778	72.222221	6	2	0	62.222221
6	3	26.666666	73.333336	6	3	26.666666	68.888885
6	4	6.666667	63.333332	6	4	6.666667	63.333332
6	5	10	43.333332	6	5	26.666666	60
6	7	6.666667	46.666668	6	7	13.333333	60
6	8	13.333333	46.666668	6	8	26.666666	60
7	0	26.666666	64.444443	7	0	28.888889	57.777779
7	1	26.666666	71.111115	7	1	26.666666	50
7	2	26.666666	77.777779	7	2	6.666667	52.222221
7	3	26.666666	57.777779	7	3	34.444443	55.555557

7	4	20	66.666664	7	4	6.666667	51.111111
7	5	33.333332	60	7	5	28.888889	46.666668
7	6	15.555555	55.555557	7	6	20	46.666668
7	8	13.333333	17.777779	7	8	33.333332	24.444445
8	0	32.222221	73.333336	8	0	15.555555	54.444443
8	1	32.222221	73.333336	8	1	15.555555	54.444443
8	2	32.222221	80	8	2	24.444445	61.111111
8	3	32.222221	73.333336	8	3	24.444445	50
8	4	25.555555	66.666664	8	4	23.333334	47.777779
8	5	38.888889	53.333332	8	5	37.777779	41.111111
8	6	18.888889	52.222221	8	6	26.666666	41.111111
8	7	18.888889	25.555555	8	7	33.333332	21.111111

Table A.2.3: Second failure analysis data for simplified PAN-European network - summary

	After second failure		After second reprovisioning	
Nodes	Unavailability	Unprotectability	Unavailability	Unprotectability
0	22.9166665	56.52777788	24.02777725	52.91666538
1	21.1111106	58.88888938	23.33333263	50.8333325
2	23.4722218	67.916667	15.55555563	53.74999963
3	25.4166664	58.05555588	31.5277775	55.416666
4	19.5833331	63.05555425	16.66666663	49.72222263
5	28.472222	54.1666665	27.5	49.3055555
6	19.0277775	64.16666738	19.30555525	50.00000025
7	21.6666666	60.27777838	22.49999963	49.3055555
8	22.2222219	56.38888938	25.83333313	51.94444463
	22.6543207	**59.93827178**	**22.9166664**	**51.46604911**

APPENDIX 3: LIST OF DEFINITIONS

- **Optical network**
  The use of light as a medium over optical fibre lines to enable communication and data to be transmitted.
- **Connection**
  A data or communication call set up between a start and destination terminal.
- **Protection**
  Pre-determined fixed backup paths set up in a network as protection against failures.
- **Restoration**
  The adaptive, failure-specific, simultaneous computation of backup routes as a response to a failure and network state.
- **Node**
  A termination point for connecting links.
- **Link**
  A single unit of bandwidth at the respective level of transport management.
- **Path**
  A concatenation of cross-connected links forming a unit-capacity digital connection between its end points.
- **Span**
  The set of all (working and spare) links between nodes that are adjacent in the physical graph.
- **Route**
  The set of span designations that is contiguous on the physical graph.
- **Working link**
  A link that is in-service, as part of a traffic-bearing path.
- **Spare link**
  An equipped but idle link available for restoration.