Survivability Strategies in all Optical Networks

UNIVERSITY OF
KWAZULU-NATAL

By
Sidharta Singh

Submitted to the Department of Electrical Engineering in partial fulfilment of the requirements for the degree of M.Sc. (Information Technology and Telecommunications)

University of KwaZulu – Natal
South Africa

Supervisor: Prof B.M.Nleya

Durban, January 2006

As the candidates supervisor I have/have not approved this Dissertation for submission

Signed :……..

Name :……..

Date :……...

Acknowledgements

Foremost I wish to thank God for his guidance. I would also like to give sincere thanks to my family especially my mother and father for all the support and encouragement they gave me during the time spent towards the successful completion of this research study.

I would also like to express my sincere gratitude to Professor B M Nleya for his assistance and excellent guidance during the course of my research. His technical knowledge and understanding of the subject provided me with a lot of insight, which enabled me to complete this research.

Abstract

Recent advances in fiber optics technology have enabled extremely high-speed transport of different forms of data, on multiple wavelengths of an optical fiber, using Dense Wavelength Division Multiplexing (DWDM). It has now become possible to deploy high-speed, multi-service networks using DWDM technology. As the amount of traffic carried has increased, any single failure can be catastrophic. Survivability becomes indispensable in such networks. Therefore, it is imperative to design networks that can quickly and efficiently recover from failures. Most research to date in survivable optical network design and operation focuses on single link failures, however, the occurrence of multiple-link failures are not uncommon in networks today. Multi-link failure scenarios can arise out of two common situations. First, an arbitrary link may fail in the network, and before that link can be repaired, another link fails, thus creating a multi-link failure sequence. Secondly, it might happen in practice that two distinct physical links may be routed via the same common duct or physical channel. A failure at that shared physical location creates a logical multiple-link failure.

In this dissertation, we conduct an intensive study of mechanisms for achieving survivability in optical networks. From the many mechanisms presented in the literature the focus of this work was on protection as a mechanism of survivability. In particular four protection schemes were simulated and their results analyzed to ascertain which protection scheme achieves the best survivability in terms of number of wavelengths recovered for a specific failure scenario. A model network was chosen and the protection schemes were evaluated for both single and multiple link and node failures. As an indicator of the performance of these protection schemes over a period of time average service availability and average loss in traffic for each protection scheme was also simulated. Further simulations were conducted to observe the percentage link and node utilization of each scheme hence allowing us to determine the strain each protection scheme places on network resources when traffic in the network increases. Finally based on these simulation results, recommendations of which protection scheme and under what failure conditions they should be used are made.

Table of Contents

Chapter 1 : Introduction to Optical Networks

Chapter 2 : DWDM Network Architectures

Chapter 3 : Wavelength Routing and Connection Management in Optical Networks

Chapter 4 : Survivability Strategies in Optical Networks

Chapter 5 : Testing and Simulation

Chapter 6 : Conclusions and Recommendations

Appendix

CD-Rom Appendix – Numerical Data

List of Figures

List of Tables

List of Abbreviations

APS	-	Automatic Protection Switching
ATM	-	Asynchronous Transfer Mode
BER	-	Bit Error Rate
BLSR	-	Bidirectional Line-Switch Ring
DEMUX	-	Demultiplexer
DIR	-	Destination Initiated Reservation
DSL	-	Digital Subscriber Line
DWDM	-	Dense Wavelength Division Multiplexing
DXC	-	Digital Cross-Connect
EDFA	-	Erbium-Doped Fibre Amplifier
FC	-	Fibre Channel
FDDI	-	Fibre Distributed Date Interface
FR	-	Frame Relay
HDLC	-	High Level Data Link Control
IP	-	Internet Protocol
IPS	-	Intelligent Protection Switching
ITU	-	International Telecommunication Union
LAN	-	Local Area Network
MAN	-	Metropolitan Area Network
MPLS	-	Multiprotocol Label Switching
MS-SPRing	-	Multiplex Section Shared Protection Ring
MUX	-	Multiplexer
OADM	-	Optical Add/Drop Multiplexer
O-APS	-	Optical Automatic Protection Switching
O-BLSR	-	Optical Bidirectional Line-Switched Rings
OCH	-	Optical Channel
OMS	-	Optical Multiplex Section
O-MSP	-	Optical Multiplex Section Protection
OMS-SPRing	-	Optical Multiplex Section Shared Protection Ring
ON	-	Optical Networking
O-LSP	-	Optical Label-Switched Path
OSNR	-	Optical Signal to Noise Ratio
OSPF	-	Open Shortest Path First protocol
OTN	-	Optical Transport Network
O-UPSR	-	Optical Unidirectional Path Switching Ring
O-UPSR	-	Wavelength Unidirectional Path Switching Ring
OXC	-	Optical Cross-Connect
PPP	-	Point-to-point protocol
p-t-p	-	Point-to-Point
QoS	-	Quality of Service
SDH	-	Synchronous Digital Hierarchy
SDL	-	Synchronous Data Link
SIR	-	Source Initiated Reservation
SLA	-	Service Level Agreement
SMF	-	Single-Mode Fibre
SONET	-	Synchronous Optical Network
SPF	-	Shortest Path First
TDM	-	Time Division Multiplexing
UPSR	-	Unidirectional Path Switched Ring
WAN	-	Wide Area Network
WDM	-	Wavelength Division Multiplexing
WXC	-	Wavelength Cross Connect

Chapter 1

Introduction to Optical Networks

In this chapter we provide a brief overview of optical networks and their different generations. We also discuss the research challenges in these networks, including the survivable network design problem and the challenges it poses. Finally, we discuss the contribution of this dissertation, and its organization.

1.1 Optical Networks: Background

One of the major issues in the networking industry today is tremendous demand for more and more bandwidth. Before the introduction of optical networks, the reduced availability of fibres became a big problem for the network providers. However, with the development of optical networks and the use of Dense Wavelength Division Multiplexing (DWDM) technology, a new and probably, a very crucial milestone is being reached in network evolution. The existing SONET/SDH network architecture is best suited for voice traffic rather than today's high-speed data traffic. To upgrade the system to handle this kind of traffic is costly. Hence there was a need for the development of an intelligent all-optical network. Such a network will bring intelligence and scalability to the optical domain by combining the intelligence and functional capability of SONET/SDH, the tremendous bandwidth of DWDM and innovative networking software to create a variety of optical transport, switching and management related products.

Besides increased bandwidth, the reliability of the network also had to be very high. Survivability refers to the ability of a network to maintain an acceptable level of service during a network or equipment failure. Mechanisms for survivability can be built at the optical transport layer or at higher network layers such as IP or ATM. The physical layer is close to most of the usual faults that occur, such as a cable cut. Survivability mechanisms in the optical layer involve detecting this and performing a simple switch to divert the traffic through an alternate path. This is called protection. Hence optical layer mechanisms are inherently faster. At a higher layer, an alternate path can be worked out on the basis of an algorithm, priority considerations can be made and the

process can be more intelligent. This is called restoration of traffic and is more time consuming than protection. Hence this mechanism cannot be used against the more common fibre cuts. It has to work along with the optical layer survivability.

Optical Fibre communication systems offer a huge bandwidth as compared to copper cables. They are also less susceptible to electromagnetic interferences. The first transatlantic optical communication system, TAT-8, was installed in 1988, operating at 140 Mbps. Since then, in almost 16 years, advances in optical communication technology have facilitated transmission speeds exceeding 1 Tbps. The advances in optical devices, and transmission systems, combined have enabled this to happen. Currently, two spectral regions, centred at 1300 nm and 1550 nm, of an optical fibre are used for transmission. Using single mode optical fibres, the effective transmission windows available at these spectral regions correspond to 14 THz and 15 THz of potential frequency space for transmission.

Increasing the transmission rates could not be adopted as the only means of increasing the network capacity. Transmission rates beyond a few tens of gigabits per second could not be sustained for longer distances for reasons of impairments due to amplifiers, dispersion, non-linear effects of fibre, and cross-talk. Hence, wavelength division multiplexing (WDM) was introduced that divides the available fibre bandwidth into multiple smaller bandwidth units called wavelengths. The WDM-based networking concept was derived from a vision of accessing a larger fraction of the approximately 50-THz theoretical information bandwidth of a single-mode fibre. A natural approach to utilize the fibre bandwidth efficiently is to partition the usable bandwidth into non-overlapping wavelength bands. Each wavelength, operating at several gigabits per second, is used at the electronic speed of the end-users. The end-stations thus can communicate using wavelength-level network interfaces. Wavelength division multiplexing turns out to be the most promising candidate for improving the fibre bandwidth utilization in future optical networks.

In literature, optical networks are categorized by dividing their evolution into two phases. First generation optical networks are those networks in which optical fibre was used as a mode of communication while all the processing happens at the electronic

level, and second generation optical networks in which some of the decisions take place in the optical domain, these are described below.

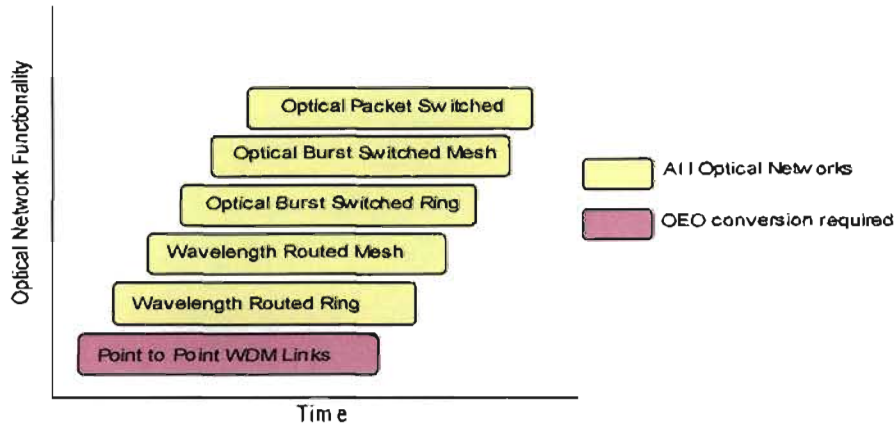


Figure 1-1 Optical network evolutions

1.1.1 First Generation Optical Networks

First generation optical networks employ fibre only as a transmission medium. These networks essentially replace copper cables with optical fibres. The key feature of first generation optical networks is that all processing is carried out in the electronic domain. The electronics at a node must handle all data intended for that node as well as all data passing through the node and destined to other nodes in the network. This essentially puts a limitation on the transmission speed of such networks due to the electronic processing bottleneck. First generation optical networks have been widely deployed in public as well as private enterprise networks. The public network standard for transmission and multiplexing incorporated in North America is Synchronous Optical Networks (SONET) and Synchronous Digital Hierarchy (SDH) in Europe. The private enterprise network standards include fibre interconnects, such as Enterprise Serial Connection (ESCON), Fibre Channel, High-Performance Parallel Interface (HIPPI), and metropolitan area networks, such as Fibre Distributed Data Interface (FDDI) [1] and Gigabit Ethernet [2].

SONET networks probably are the most popular among first generation networks. They incorporate a wide variety of functions. For example, they provide point-to-point connections between different node pairs in the network. They also provide add/drop

functionalities, such that only a part of the streams are dropped at a node, and the rest can pass through. SONET networks consist of cross-connects, which can switch multiple traffic streams. More-over, one of the most attractive features of SONET networks is their fault tolerant capability, wherein they handle node and link failures without disrupting the services.

1.1.2 Second Generation Optical Networks

The first generation optical networks are now getting in place. An increasing realization that optical networks are capable of providing more functions than just point-to-point transmission led to the emergence of second generation optical networks. Second generation optical networks use WDM technology to split the huge bandwidth provided by a fibre into multiple wavelength channels, that can be used to support multiple transmissions simultaneously. Also, some of the switching and routing functions that are performed by the electronics in first generation optical network can be carried out in the optical domain in second generation optical networks. Second generation optical networks offer different types of services to the higher network layers. The most commonly used service is the light path service. A light path is a dedicated connection on a wavelength between two nodes in the network, such that no electronic conversion takes place on the path between these two nodes. Moreover, second generation optical networks offers transparency, i.e., they are insensitive to the nature of the coding or modulation techniques used over the light paths.

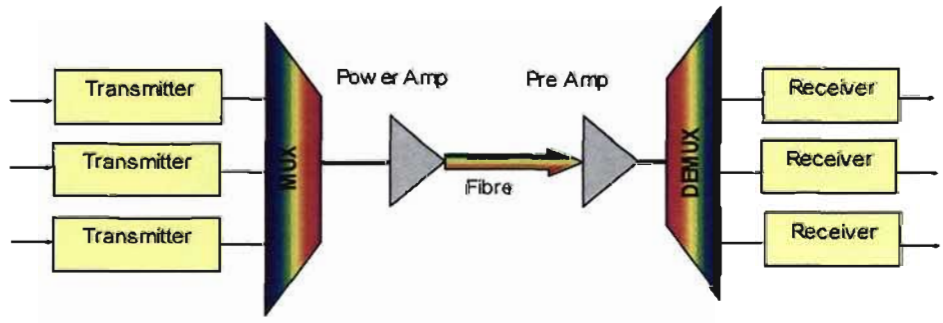


Figure 1-2 A typical WDM link.

Since, second generation optical networks employ WDM technology, they are also known as WDM networks. A typical WDM link is shown in Figure 1-1. It consists of a

set of transmitters, optical amplifiers and receivers. The transmitters are lasers, each supporting one wavelength. The outgoing signals from different transmitters are multiplexed together using a multiplexer. The power amplifier immediately after the multiplexer amplifies the combined signal. The signal after travelling some distance on fibre may need amplification again due to attenuation; this task is carried out by an amplifier. Finally, at the destination, the combined signal is amplified again and demultiplexed. Due to demultiplexing, the signal is split into different wavelengths which are converted to the electronic domain using photodetectors, where each photodetector is tuned to a specific wavelength.

1.2 Optical Networking: IP over DWDM

The telecommunication field has a variety of standards defining different layers for the whole infrastructure. In the past, the end users were people making phone calls or using fax machines etc. However, according to the current understanding, it seems that in the future almost all the traffic will be IP-based. The evolution will tend towards IP-over-WDM networks, for which several alternative approaches have been proposed in the literature [3].

'Internet Protocol (IP) over DWDM' is the concept of sending data packets over an optical layer using DWDM for its capacity and other operations. In the modern day world, the optical layer has been supplemented with more functionality, which was once in the higher layers. This creates a vision of an all-optical network where all management is carried out in the photonic layer. The optical network is proposed to provide end-to-end services completely in the optical domain, without having to convert the signal to the electrical domain during transit.

Transmitting IP directly over DWDM has become a reality and is able to support bit-rates of OC-192 (Fibre optic connection capable of transferring data at 9.952 Gbps). As we can clearly see, it holds the key to the bandwidth issue. In first generation optical networks the physical layer is merely an optical fibre providing a single wavelength. In second generation optical networks, the physical layer is much more intelligent and is capable of providing many services. The role of the second generation optical networks is defined by the services that can potentially be offered to users. The network can be

viewed as different layers interoperating with each other, as shown in Figure 1-2. Different carriers, depending on their requirements can choose different ways to realize the network. We would be mostly looking at the optical layer from the protection services perspective that needs to be provided by the optical layer to the higher layers. The IP, ATM and SONET layers all incorporate their own protection and restoration mechanisms. These layers are designed to interoperate with other layers and can also directly operate with the fibre. Network service providers can offer varying classes of service based on the choice of protection which can vary from full protection to no protection. Hence, based on the service classes, the traffic in the network can be divided into three classes, full protection, no protection and best-effort. Full-protection traffic is usually the high-priority traffic which requires complete protection at the optical layer. There may be a second category of carriers, which support high priority traffic but requires no protection at the optical layer, as they might be protected by some higher layers such as SONET. The best-effort class attempts to provide protection for the connections based on the resources available. This may include the IP traffic which have their own protection mechanisms that are slower, and in which cases the optical layer protection maybe beneficial.

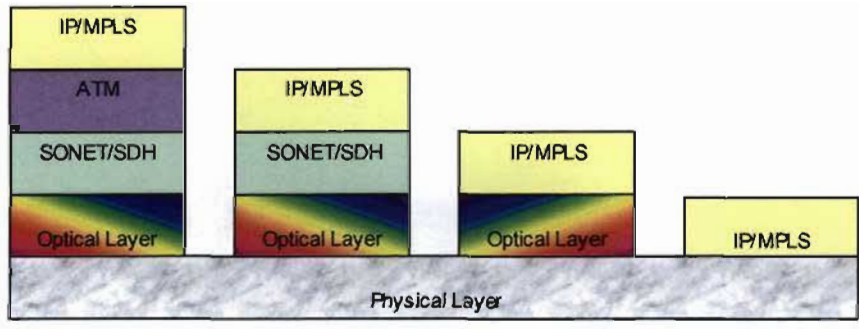


Figure 1-3 Possible Layering Architectures

In Figure 1-3, some of the possible layering alternatives are depicted. Consider first the IP over ATM over SONET/SDH over optical solution. Roughly speaking the role of each layer from bottom to top is as follows:

- Physical layer provides the optical fibres between the network nodes including possible optical fibre amplifiers.

- Optical layer provides transparent all-optical light paths between node pairs for a higher layer. Each physical link (or fibre) is capable of carrying several light paths using WDM technology, and each light path corresponds to an optical link for the SONET/SDH node.

- SONET/SDH layer provides constant bit rate transmission pipes from point A to point B over the SONET/SDH network. Furthermore, SONET/SDH network's protection and restoration capabilities can be used to ensure effectively uninterrupted bit flows.

- ATM layer can be used to provide virtual connections (VC) of arbitrary bit rate from point A to point B with different QoS parameters. ATM can be used for traffic engineering purposes, but it has become somewhat redundant as IP/MPLS routers tend to provide similar features.

- IP/MPLS layer only expects transmission links for IP packets. Each additional layer naturally brings some extra overhead to the transmission. Hence, the typical IP over ATM over SONET/SDH over WDM mapping can be considered to be an inefficient solution. Eventually the trend is towards IP-over-Optical solutions, where IP packets are transferred directly on the optical layer without any intermediate layer, i.e. IP/MPLS over WDM solution.

For completeness, Figure 1-4 tries to illustrate the currently used solutions to carry IP traffic using an underlying WDM network.

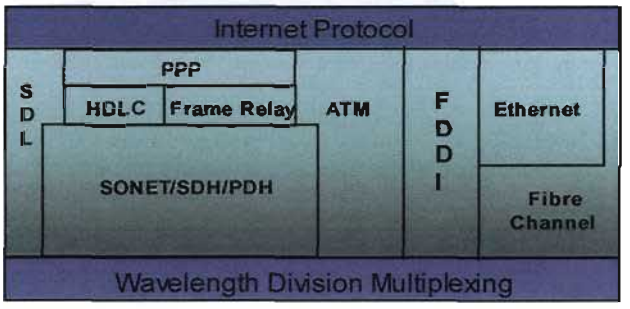


Figure 1-4 Different approaches for IP-over-Optical (WDM)

Also in the IETF work is going on for standardizing the so-called generalized multi protocol label switching (GMPLS), which is supposed to unify the management of the optical networks and allow interoperability between different manufacturers.

1.3 Research Challenges in Survivable WDM Optical Networks

There are various challenges that survivable WDM optical networks pose, in this section we discuss major difficulties regarding the design and operation of survivable WDM networks. Under the heading of WDM network, we will cover only wavelength routed networks and not broadcast and select networks. Generally the design of a WDM network is an of-line activity, where a designer is supplied with a projected static traffic matrix and is required to design and provision the corresponding WDM network that realizes the traffic matrix while meeting an objective, which maybe minimizing the cost of the network. Alternatively, the network architecture is given and the task is either to fully accommodate the given traffic matrix using the least number of network resources, or to maximally accommodate the given matrix using available resources. In contrast to designing, operation of a survivable WDM network is an on-line activity in which the network has already been designed and most probably supporting some traffic. The task here is to either accommodate as many new traffic requests while optimizing the network resource usage, or to accommodate all the new traffic with a minimum number of additional resources. The distinct classification of each problem into off-line and on-line, however, is sometimes blurred. The design and operation of the WDM networks basically addresses the following issues:

- For a given amount of resources, how much traffic can be accommodated?
- How much resources are needed to fully accommodate a given traffic matrix?
- How to route and assign wavelengths to traffic requests in a way that satisfies a certain objective function?
- How to provide protection to either all or critical traffic requests, while achieving some objective, such as optimization of network resources?

Numerous methods have been proposed for joint working and spare capacity planning in survivable WDM networks [4, 5, 6]. These methods consider a static traffic demand and optimize network cost assuming various cost models and survivability paradigms.

However none of these approaches study the incremental network upgrade problem. Some ILP formulations have been studied for the incremental network upgrade problem. However the ILP techniques have limitations in its applicability in large networks with huge traffic demands. We briefly discuss some issues and challenges that arise in the design and operation of the mesh-restorable WDM Networks. This type of network is of interest to us since it will be used in the simulations, hence understanding these issues will assist in the analysis and explanations of possible errors.

1.3.1 Logical Topology Design Problem

Generally, the capacity requirements for data flows (packet flows) are not integer multiples of the capacity of a single wavelength channel, but arbitrary multiples or fractions of that capacity. Furthermore, these flows can be aggregated at any node to a single flow and later split again at some intermediate node and then forwarded to other directions.

By a multihop network we mean a network where each data flow uses possibly more than one optical hop. This causes an extra processing load for the intermediate nodes and increases the delays packets experience, but makes possible more efficient use of the optical resources. The aggregation process corresponds to routing at the logical layer. It is not usually practical to configure the network so that the logical and physical layers are topologically equivalent, because then the conversion between layers causes unnecessary delays to the traffic. The problem of deciding on both the light path establishment and the routing at the logical layer is often referred to as the logical topology design problem (LTD), or the Multihop Network Configuration Problem.

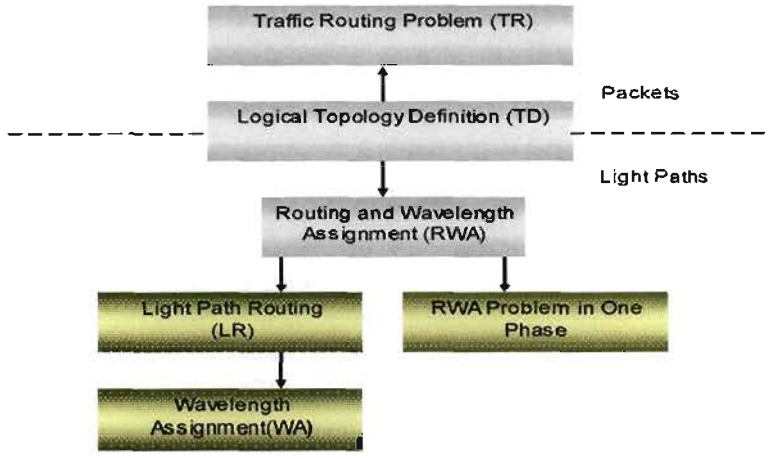


Figure 1-5 Hierarchical model of WDM network configuration

This kind of problem can be solved in a hierarchical way, as presented in Figure 1-5. At the first step, current (average) data streams between the nodes are mapped to light path requests, i.e. the requirements for the logical topology are set (topology definition, TD). If there are enough resources available in the network, each light path request can be fulfilled and a feasible solution has been found.

A common approach is to first fix the logical topology and packet level routing, i.e. the TD and TR problems in Figure 1-5. This step essentially defines the light paths each packet uses to travel through the network towards the destination node. Once this decision has been made, the problem is reduced to the establishment of light paths in the network (the third box from the top in Figure 1-5). In summary, the TD step defines a set of light path requests, i.e. by using the mean traffic flows between the node pairs (and possibly the knowledge about physical network) as an input it determines the number of light paths to be established between each node pair, which allows, in some sense, the most efficient transmission of data packets. The light path establishment step gets the light path requests (number of light paths to be established between each node pair) as an input and determines a feasible route and wavelength for each request.

The establishment of light paths in the network, i.e. the routing and wavelength assignment problem (RWA) is traditionally solved in one or two phases. In a one-phase

solution both the route (for the light path) and its wavelength(s) are determined simultaneously.

Alternatively the RWA problem can be further decomposed into light path routing (LR) and wavelength assignment (WA) steps. In this two-phase solution the path is first fixed for each light path and then a feasible wavelength is assigned to each light path, shorter paths are usually good candidates.

1.3.2 Routing and Wavelength Assignment

The Routing and Wavelength Assignment (RWA) problem is deemed as: *given a network topology, a set of end-to-end light path requests, determine how to route those requests, and which wavelengths they should be assigned using the minimum possible number of wavelengths* [7]. Sometimes routing is either given or is straight forward, e.g., in a unidirectional ring. In such cases, the RWA problem reduces to solving the wavelength assignment problem only. The wavelength assignment for a network must satisfy two constraints, namely,

- no two light paths on the same physical link be assigned the same wave
- if wavelength conversion is not available, then wavelength continuity constraints on all the links that a light path traverses

1.4 Survivability

Survivability of a network refers to a network's capability to provide continuous service in the presence of failures. In a WDM network, as a single channel may be carrying tens of gigabits of data per second, a single failure would cause a huge amount of service disruption to a large number of users. Design of survivable WDM networks has therefore attracted the attention of the research community. The basic types of failures in the network can be categorized as either link or node failures.

Link failure usually occurs because of cable cuts, while node failure occurs because of equipment failure at network nodes. Channel failures are also possible in WDM networks. A channel failure is usually caused by the failure of transmitting and/or receiving equipment operating on that channel (wavelength). The restoration schemes differ in their assumption about the functionality of cross-connects, traffic demand,

performance metric, and network control. Survivability paradigms are classified based on the following;

- re-routing methodology as path/link based
- execution mechanisms as centralized/distributed
- computation timing as precomputed/real time,
- capacity sharing as dedicated/shared.

There are two commonly used protection schemes: shared path protection and dedicated path protection. In case of shared path protection, spare capacity is shared among different protection paths, while in dedicated path protection, the spare capacity is dedicated to individual protection paths. Shared path protection, although more difficult to implement, have been proven to be more capacity efficient than dedicated path protection.

1.4.1 Proactive Versus Reactive Restoration

A pro-active or reactive restoration method is either link based or path based. In a special case, segment based approach can also be used. In a segment based de-touring, a backup segment is assigned for more than one link. A link may be covered by more than one segment. The restoration path, as shown in Figure 1-6, is computed for each path. In case of a link failure, the backup segment is used.

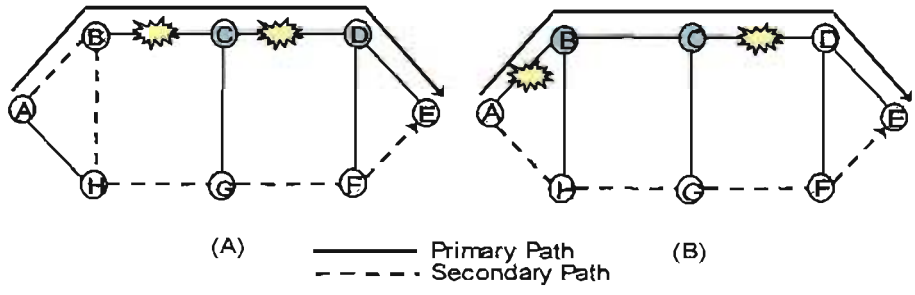


Figure 1-6 Segmented Path Protection

Link based restoration methods re-route disrupted traffic around the failed link, while path based re-routing replaces the whole path between the source and destination of a demand. Thus, a link based method employs local de-touring while the path based method employs end-to-end de-touring. De-touring mechanisms are shown in Figure1-7 and Figure1-8. For a link based method, all routes passing through a link are transferred to a local re-routing path that replaces that link. While this method is attractive for its local nature, it limits the choices for alternatives.

In case of wavelength selective networks, the backup path must use the same wavelengths for existing requests as that of their corresponding primary paths as the working segments are retained.

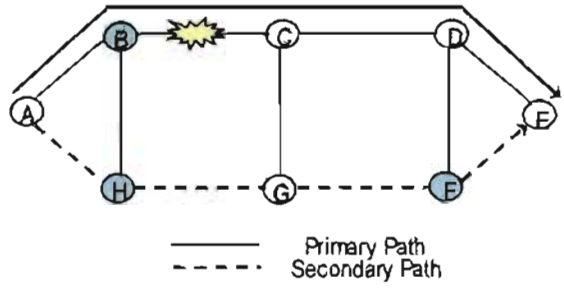


Figure 1-7 Path Based Restoration

The protection approaches are classified as 1+1, 1:1, and 1: *N* to represent the number of the entities reserved for protection. For example, in a 1+1 protection scheme, the signal is sent simultaneously over two disjoint light paths. The receiver receives the signal from both light paths and selects the better one.

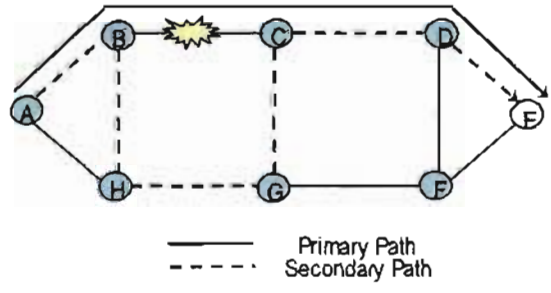


Figure 1-8 Link-Based Restoration

In a 1:1 protection scheme each primary light path has a dedicated backup light path; however, the backup light path is used only in a case of failure. In 1: N protection scheme, N primary light paths share a common backup light path. The necessary condition in this case, is that all the N light paths do not have any overlapping links. In WDM systems, due to the availability of multiple wavelengths on a single fibre, protection methods can be more flexible. This, however, makes the problem more complicated. WDM networks provide survivability by providing fault-tolerance at the optical layer. However, this has its own merits and demerits. In the following statements, we provide a brief account of such aspects paying particular attention to the optical layer.

- Optical layer protection and restoration may be used to provide an additional level of resilience in the network. For example, many transport networks are designed to handle a single failure at a time, but not multiple failures. Optical restoration can be used to provide resilience against multiple failures

- Some of the layers operating above the optical layer may not be fully able to provide all the protection functions needed in the network, hence optical layer survivability techniques can fill this deficiency.

- Optical layer protection can be more efficient at handling certain types of failures, such as fibre cuts. Handling such failures at a higher layer, say SONET, will overwhelm the network as a large number of SONET connections need to be restored.

- Optical layer protection cannot handle all types of faults in the network. For example, it cannot handle the failure of an IP router or a SONET ADM attached to the optical network.

- The optical layer protects traffic in units of light paths. Thus owing to its transparency, the optical layer cannot provide different levels of protection to

different parts of the traffic being carried on a light path (part of the traffic may be high-priority, while others may be of low-priority).

Considerable research needs to be done to understand the interactions of recovery protocols that operate at multiple layers in the event of a fibre failure. The outage durations in the event of a failure, could be lengthened as recovery protocols from various layers might interact with each other. The network might end up in a deadlocked state never converging to a new topology.

1.5 Contributions and Organization of Dissertation

In this dissertation we investigate the various protection strategies that can be used to improve survivability in optical networks we also attempt to address some of the challenges discussed in Section 1.3. Our approach is to start with simple models and evolve into more complex but realistic models for the design and provisioning of WDM network. We propose suitable protection schemes for the design of survivable optical networks. One of the main thrust of our work is to develop more realistic and generic models and provide solutions for designing networks which are resilient to multiple failures arising out of shared resources and component failures.

The rest of the dissertation is organized as follows. In Chapter 2, we provide an overview of related literature on architectures in WDM optical networks. In Chapter 3, we address the issue of wavelength routing and connection management in optical networks, the different wavelength routing schemes are classified accordingly and the overflow model is discussed. A justification of the suitable wavelength schemes is made from results obtained in the literature. In Chapter 4, we discuss survivability strategies in optical networks; here we classify the various types of failures and also look at ITU-T recommendations for survivability in optical networks. The various protection schemes are also discussed and their role in the various layers is presented. Chapter 5, we propose a model for simulation purposes, this model is used under varying failure scenarios and the relevant protection schemes are evaluated accordingly. The main focus of this chapter is to obtain results on the efficiency of the various protection schemes in order to ascertain their robustness under various failure scenarios. In Chapter 6 we conclude this dissertation and outline future research directions in the field of survivable network design in WDM networks.

Chapter 2

DWDM Network Architectures

Various architectures exist in optical networks these can be split into three distinct classes namely: broadcast-and-select networks, wavelength routed networks, and linear lightwave networks. This chapter provides a detailed explanation of each type of network and in some instances examples are provided to demonstrate how they operate.

2.1 Broadcast-and-Select Networks

A broadcast-and-select network consists of a passive star coupler connecting the nodes in the network as shown in Figure 2-1, each node is equipped with one or more fixed-tuned or tuneable optical transmitters and one or more fixed-tuned or tuneable optical receivers. Different nodes transmit messages on different wavelengths simultaneously. The star coupler combines all these messages and then broadcasts the combined message to all the nodes. A node selects a desired wavelength to receive the desired message by tuning its receiver to that wavelength. Note that the star coupler offers an optical equivalent to radio systems: each transmitter broadcasts its signal or message on a different wavelength and the receivers are tuned to receive the desired signal.

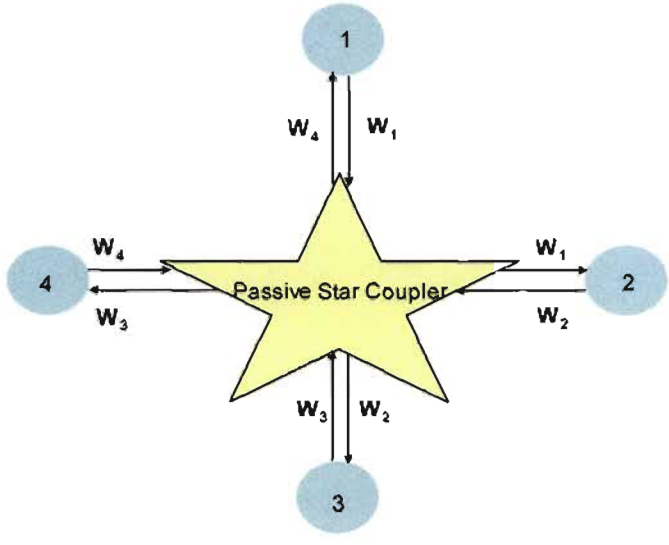


Figure 2-1 Broadcast and Select Network

A $N \times N$ star coupler can be realized using a multistage interconnection network which has $log_2 N$ stages of 2×2 couplers with $N/2$ couplers per stage (assuming N is a power of 2) or directly in integrated optics form with a common coupling region. Integrated optics refers to integration of optical components with fiber interconnections onto a single optical substrate, similar to the way in which electrical components (such as resistors, capacitors, and inductors) are combined in an electronic integrated circuit.

In single-hop broadcast-and-select networks, a message, once transmitted as light, reaches its final destination directly, without being converted to electronic form in between. In order to support packet switching in these networks, we need to have optical transmitters and receivers that can tune rapidly. This is because, in a packet-switched network, a node must be able to transmit (receive) successive packets to (from) different nodes on different wavelengths.

The main networking challenge in these networks is the coordination of transmissions between various nodes. In the absence of coordination or efficient medium access control (MAC) protocol, collisions occur when two or more nodes transmit on the same wavelength at the same time. Also, destination conflicts occur if two or more nodes transmit on different wavelengths to the same destination when the destination has only one tuneable optical receiver. Moreover, the destination must know when to tune to the appropriate wavelength to receive a packet. Several MAC protocols have been proposed to prevent such collisions/conflicts for single-hop broadcast-and-select networks, assuming the availability of rapidly tuneable transmitters and/or receivers. To support packet switching efficiently in broadcast-and-select networks, a multihop approach, which avoids rapid tuning altogether, can be used. Each node has a small number of fixed-tuned optical transmitters and fixed-tuned optical receivers. Each transmitter is at a different wavelength. We can represent the network as a graph, wherein a node corresponds to a network node and an edge corresponds to a transmitter–receiver pair on the same wavelength. Thus we obtain a virtual or logical topology over the physical broadcast topology. Figure 2-1 shows a four-node broadcast-and-select network. Each node transmits at one fixed wavelength and receives on one fixed wavelength. For example, node 1 can transmit directly to node 2 using wavelength w_1, but not to node 3. To transmit to node 3, node 1 sends a packet to node 2 on wavelength w_1, which

receives it, converts it to electronic form, and retransmits it on wavelength w_2. The packet then reaches node 3.

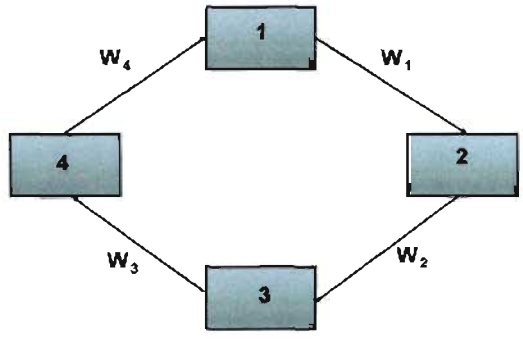


Figure 2-2 Logical topology of Broadcast and Select Network

The virtual topology of the network in Figure 2-1 is shown in Figure 2-2. In these networks, a packet may have to go through more than one hop before reaching its destination. This leads to an increase in propagation delay in addition to queuing delays at intermediate nodes, and wastage of network capacity. The advantage of broadcast-and-select networks is in their simplicity and natural multicasting capability (ability to transmit a message to multiple destinations). However, they have severe limitations:

- They require a large number of wavelengths, typically at least as many as there are nodes in the network, because there is no wavelength reuse in the network. Thus the networks are not scalable beyond the number of supported wavelengths.
- They cannot span long distances since the transmitted power is split among various nodes and each node receives only a small fraction of the transmitted power, which becomes smaller as the number of nodes increases. For these reasons, the main application for broadcast-and-select is high-speed local area networks (LANs) and metropolitan area networks (MANs).

2.2 Wavelength Routed Networks

Wavelength routed WDM networks have the potential to avoid the three problems-lack of wavelength reuse, power splitting loss, and scalability to wide area networks (WANs)-of broadcast-and-select networks. A wavelength routed network consists of

WXCs (routing nodes) interconnected by point-to-point fiber links in an arbitrary topology. Each end node (end user) is connected to a WXC via a fiber link. The combination of end node and its corresponding WXC is referred to as a (network) node. Each node is equipped with a set of transmitters and receivers, for sending data into the network and receiving data from the network, respectively, both of which may be wavelength-tuneable.

In a wavelength routed network, a message is sent from one node to another node using a wavelength continuous route called a lightpath, without requiring any optical-electronic-optical conversion and buffering at the intermediate nodes. This process is known as wavelength routing. Note that the intermediate nodes route the lightpath in the optical domain using their WXCs. The end nodes of the lightpath access the lightpath using transmitters/receivers that are tuned to the wavelength on which the lightpath operates. A lightpath is an all-optical communication path between two nodes, established by allocating the same wavelength throughout the route of the transmitted data.

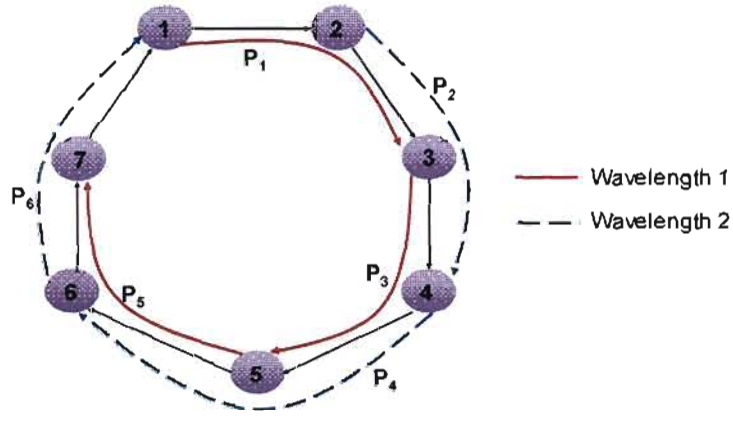


Figure 2-3 Wavelength Routed Network

Thus it is a high-bandwidth pipe, carrying data up to several gigabits per second, and is uniquely identified by a physical path and a wavelength. The requirement that the same wavelength must be used on all the links along the selected route is known as the wavelength continuity constraint. Two lightpaths cannot be assigned the same

wavelength on any fiber. This requirement is known as distinct wavelength assignment constraint. However, two lightpaths can use the same wavelength if they use disjoint sets of links. This property is known as wavelength reuse.

Example 1: Consider a wavelength routed network with seven nodes and two wavelengths per fiber as shown in Figure 2-3. Assume that lightpaths are to be established one for each of the node pairs <1, 3>, <2, 4>, <3, 5>, <4, 6>, <5, 7>, <6, 1> and < 7, 2 > . Further assume that every node is equipped with one transmitter and one receiver. For the given set of node pairs, a node is a source for one lightpath and destination for one lightpath. There exists only one physical path between any node pair. Every fiber link in the network would carry physical paths corresponding to two lightpaths, if lightpaths were successfully established for all the given node pairs. Since two wavelengths are available on any fiber link, it should be possible to route all the lightpaths. However, due to the wavelength continuity constraint it is not possible to establish lightpaths for all seven node pairs.

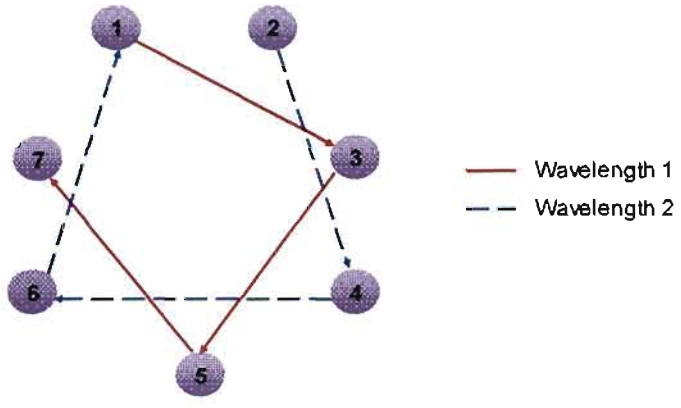


Figure 2-4 Logical Topology of Wavelength Routed Network

The Figure 2-4 shows a possible way of routing six lightpaths p1, p2, p3, p4, p5, p6 where p_i is the lightpath emanating from node i. Since p_1 uses wavelength w_1, p_2 can use only w_2, as p_1 and p_2 share a link. Lightpath p_3 can use only w_1, as p_2 and p_3 share a link. Lightpath p_4 can use only w_2, as p_3 and p_4 share a link. Lightpath p_5 can use only w_1, as p_4 and p_5 share a link similarly lightpath p_6 can use only w_2, as p_5 and p_6 share a link. As a consequence, wavelength w_2 is free on link $7 \rightarrow 1$ and w_1 is free on link $1 \rightarrow 2$.

Therefore, a lightpath cannot be established from node 7 to node 2 even though bandwidth (wavelength) is available on links $7 \rightarrow 1$ and $1 \rightarrow 2$, a transmitter is available at node 7, and a receiver is available at node 2. As we will see later, this bandwidth loss caused by the wavelength continuity constraint can be overcome by using a wavelength converter. However, observe that both the wavelengths w_1 and w_2 are reused two times, thus helping increase the number of lightpaths established while employing a limited number of wavelengths.

Wavelength reuse refers to simultaneous transmission of messages on the same wavelength over fiber-link-disjoint lightpaths; this feature of wavelength routed networks makes them more scalable than broadcast-and-select networks. Another important characteristic which enables wavelength routed networks to span long distances is that the transmitted power invested in the lightpath is not split to irrelevant destinations. Given a WDM network, the problem of routing and assigning wavelengths to lightpaths is of paramount importance in these networks, and clever algorithms are needed in order to ensure this function (routing and wavelength assignment) is performed using a minimum number of wavelengths. The number of available wavelengths in a fiber link plays a major role, in these networks, which currently varies between 4 and 32, but is expected to increase.

Packet switching in wavelength routed networks can be supported by using either a single-hop or a multi-hop approach, in a way similar to broadcast-and-select networks. In the multi-hop approach, a virtual topology (a set of lightpaths or optical layer) is imposed over the physical topology (which is not broadcast here) by setting the WXCs in the nodes. Over this virtual topology, a packet from one node may have to be routed through some intermediate nodes before reaching its final destination. At each intermediate node, the packet is converted to electronic form and retransmitted on another wavelength. A virtual topology, formed by lightpaths p_1 through p_6, corresponding to the physical network shown in Figure 2-3, is given in Figure 2-4. A packet from node 3 (source) is routed through intermediate node 0 undergoing optical-electronic-optical conversion at this node before reaching node 2 (destination).Existing Internet backbone networks consist of high-capacity IP (Internet Protocol-developed for providing connectionless transfer of packets across an internetwork) routers interconnected by point-to-point fiber links. Traffic is transported between routers

through high-speed gigabit links. These links are realized by SONET or ATM-over-SONET technology. The backbone routers use IP-over-SONET or IP-over-ATM-over-SONET technology to route IP traffic in the backbone network. Most of the SONET-based backbone transport networks provide data interface at the rate of OC-3 and OC-12. The traffic demand is growing at a faster rate and a point has been reached where data interfaces at the rate of OC-48 and more are required. Upgrading the existing SONET transport infrastructures to handle these high-capacity interface rates is not desirable, as it is impractical to go for upgrading every time the interface rate increases. Also, such upgrading is not economical. A viable and cost-effective solution is to use WDM technology in backbone transport networks.

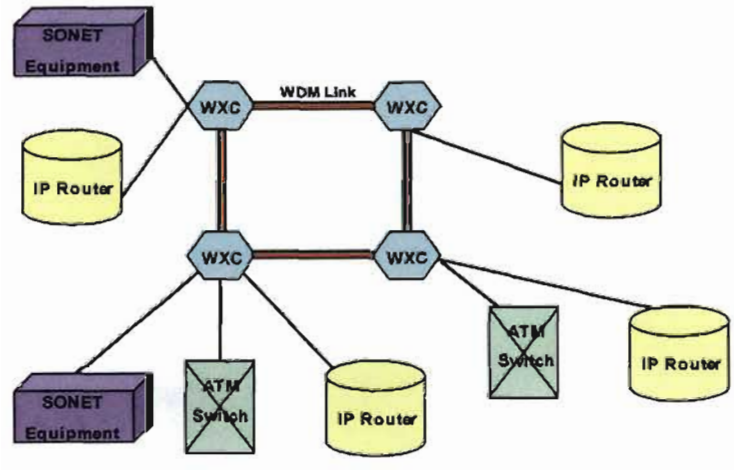


Figure 2-5 WDM Backbone Network

In such (for example, IP-over-WDM) networks, network nodes are interconnected by WDM fiber links (where each link is capable of carrying multiple signals simultaneously, each on a different wavelength), and the nodes employ WXCs and electronic processing elements. Figure 2-5 shows a typical WDM backbone network. The electronic processing element can be an IP router, ATM switch, or a SONET system.

Any two IP routers in this network can be connected together by a lightpath. Two nodes that are not connected directly by a lightpath communicate using multihop approach, i.e., by using electronic packet switching at the intermediate nodes. This electronic packet switching can be provided by IP routers, ATM switches, or SONET equipment, leading

to an IP-over-WDM or an ATM-over-WDM, or a SONET-over-WDM network, respectively.

A WDM-based transport network can be decomposed broadly into three layers, a physical media layer, an optical layer, and a client layer, as shown in Figure 2-6.

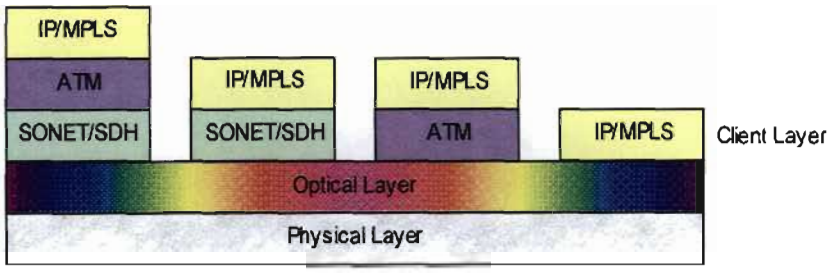


Figure 2-6 Possible layers in a WDM optical transport network.

Application of WDM technology has introduced the optical layer between the lower physical media layer and upper client layer. A set of lightpaths constitutes the optical layer (virtual topology). The optical layer provides client-independent or protocol-transparent circuit-switched service to a variety of clients that constitute the client layer. This is possible because the lightpaths can carry messages at a variety of bit rates and protocols. Thus the optical layer can support a variety of clients concurrently. For example, some lightpaths could carry SONET data, whereas others could carry IP packets/datagram's or ATM cells. A network with an optical layer can be configured such that in the event of failures, lightpaths can be rerouted over alternate paths automatically. This provides a high degree of reliability in the network. According to International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) Recommendation G.872, an optical layer can be further decomposed into three sub layers: an optical channel layer, an optical multiplex section layer, and an optical transmission section layer. The functionality of the optical channel layer is to provide end-to-end networking of optical channels (lightpaths) for transparently conveying the client data. The optical multiplex section layer concerns networking of aggregate multiwavelength optical signals. The optical transmission section layer concerns the transmission of optical signals on different kinds of optical media such as single-mode and multimode transmission.

These attractive features-wavelength reuse, protocol transparency, and reliability-make wavelength routed networks suitable for WANs. Designing an optical layer to meet the traffic demand is an important problem in order to use the wavelength and fiber resources efficiently and to provide quality service to the users. Reconfiguring the optical layer is necessitated by the changing traffic demand. Since a huge amount of traffic is carried by the optical layer, rapid service recovery in case of network component failures is critically important.

2.3 Linear Lightwave Networks

The optical spectrum can be partitioned into a number of either wavelengths or wavebands as shown in Figure 2-7. Observe that in Figure 2-8 each waveband is further subdivided into a number of wavelengths. Note that sufficient spacing or guard bands have to be placed between any two wavelengths to allow for imprecision and drift in laser transmitter tuning and to make it possible to separate adjacent signals at the receivers.

The spacing between two wavelengths or frequencies in a WDM system is referred to as channel spacing. The relationship between frequency and wavelength [1] can be obtained as follows

$$f = \frac{c}{\lambda} \qquad 2.1$$

Differentiating this equation around the centre frequency λ_0, we obtain the relationship between frequency spacing Δf and the wavelength spacing $\Delta\lambda$ as

$$\Delta f = -\frac{c}{\lambda_0^2}\Delta\lambda \qquad 2.2$$

This relationship is accurate as long as the wavelength (or frequency) spacing is small compared to the actual channel wavelength (or frequency), which is normally the case in optical communication systems. At a wavelength λ_0=1550nm, a wavelength spacing of 0.8nm corresponds to a frequency spacing of 100GHz, a typical spacing in WDM systems.

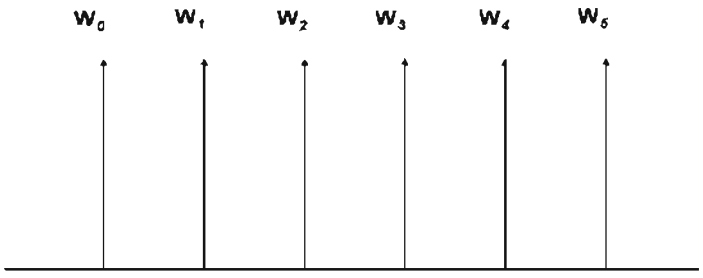


Figure 2-7 Wavelength Partitioning

Wavelength routed networks use wavelength (one-level) partitioning and in these networks several wavelengths are multiplexed on a fiber link. Linear lightwave networks, on the other hand, use waveband (two-level) partitioning, and in these networks several wavebands are multiplexed on a fiber and several wavelengths are multiplexed on each waveband. In a wavelength routed network, routing nodes demultiplex, switch, and multiplex wavelengths, whereas in a linear lightwave network, routing nodes demultiplex, switch, and multiplex wavebands, but not wavelengths within a waveband. Thus the hardware requirements at the nodes, by grouping a set of wavelengths into a waveband, in linear lightwave networks get simplified because the number of optical switches required in a node is equal to the number of wavebands, not the number of wavelengths. Since a linear lightwave network as a whole does not distinguish between wavelengths within a waveband, individual wavelengths within a waveband are separated from each other at the end nodes (optical receivers).

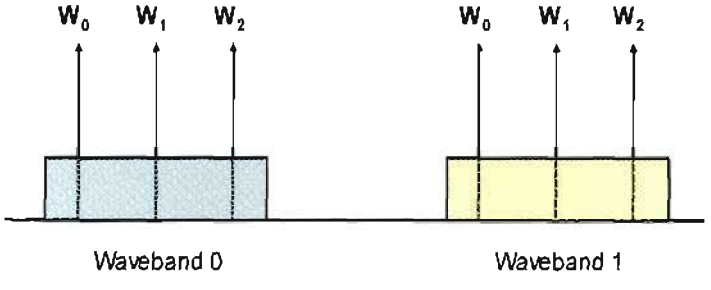


Figure 2-8 Waveband partitioning

Two constraints-wavelength continuity and distinct wavelength assignment-on optical connections applicable to wavelength routed networks also apply to linear lightwave

networks. Further, there are two routing constraints unique to linear lightwave networks:

- inseparability
- distinct source combining, that is, on any fiber, only signals from distinct sources are allowed to be combined.

2.3.1 Inseparability

This constraint can be formally defined as follows, channels belonging to the same waveband when combined on a single fiber cannot be separated within the network Figure 2-9 illustrates the inseparability constraint. Here nodes 0 through 5 are end nodes, while nodes *A* through *H* are routing nodes. The figure also shows two connections, one between nodes 0 and 2, and the other between nodes 1 and 4. The notation $< x, y >$ is used to denote a connection from node x to node y. $< 0, 2 >$ passes through nodes A, B, E, F and H, while $< 1, 4 >$ passes through nodes A, B, D and G.

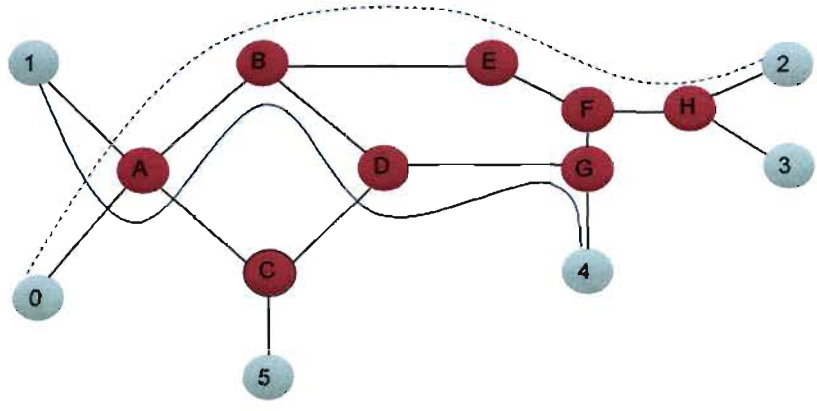


Figure 2-9 Linear Lightwave Network showing Inseparability

Since the two connections share the fibre $A \rightarrow B$, they have to use different wavelengths (because of the distinct wavelength assignment constraint). Suppose wavelength w_0 is used for $< 0, 2 >$ and wavelength w_1 for $< 1, 4 >$. The two signals, though on different wavelengths, may be in the same waveband. The two signals (that is, the power from both sources, nodes 0 and 1) are combined at node *A*. At node *B*, however, the two signals cannot be separated since they belong to the same waveband. Therefore, to route the two connections to their destinations, the combined signal power is split equally

between the output ports of node B, one leading to node E and the other to routing node D. Only the end nodes (destinations), 2 and 4, filter out $w0$ and w_1, respectively, rejecting the other wavelength. Note that some unintended destinations appear, node 2 in the case of connection $<1,4>$ and node 4 in the case of connection $<0,2>$ .These unintended destinations are called fortuitous destinations; they tend to waste fibre resources and power, and are therefore to be dispensed with, if possible. For example, in this case the fortuitous destinations could have been avoided by rerouting connection $<1,4>$ on the path 1-A-C-D-G-4.

2.3.2 Distinct Source Combining

Distinct source combining disallows an optical signal from splitting at a node, taking multiple paths in the network, and then recombining with itself. We now illustrate how a correct but poor routing algorithm can violate the distinct source combining constraint. Consider the network shown in Figure 2-9. Suppose that when two connections 0-A-B-E-F-H-2 and 1-A-B-D-G-4, on wavelengths w_0 and w_1, respectively, are in progress, a new connection $<5,3>$ is routed along the path 5-C-D-G-F-H-3 using a wavelength w_2. All three connections are assumed to be in the same waveband. Due to inseparability, signal generated at source 5 carries with it (fortuitously) portions of signals generated at sources 0 and 1 after combining with them on fibre $D \rightarrow G$. This causes the signal generated at source 0 (which split at node B) to recombine with itself on fibre $F \rightarrow H$, violating the distinct source combining constraint. Thus the new connection $<5,3>$ must not be routed along the path 5-C-D-G-F-H-3 . However, this problem could have easily been avoided had the choice of routes been more prudent. Routing connection $<1,4>$ via A, C, D and G , or routing connection $<5,3>$ via nodes C, D, B, E, F and H would have made it possible for all three connections to be routed successfully.

Setting up connections with the above routing constraints in a linear lightwave network is significantly more complicated when wavebands contain more than one wavelength. Apart from this, the combining and splitting losses present at the nodes is preventing linear lightwave networks from becoming practical. Since at each node the power at an output port is a linear combination of the powers at the input ports, these networks are called linear lightwave networks.

Chapter 3

Wavelength Routing and Connection Management in Optical Networks

At the physical layer, a complete overhaul of existing networks is envisaged from electronic media (such as twisted-pair and cable) to optical fibers. Optical fibers employing the promising technique of wavelength division multiplexing (WDM) can support around 1000 times the capacity of their electronic counterparts, by allowing the simultaneous transmission of several channels on the same fiber each on a different wavelength (frequency). In order for this method of transmission to be effective, efficient wavelength routing and connection management strategies have to be implemented. Although these topics are outside the scope of this work, they do play a part in network survivability and hence in this chapter an overview of them is presented.

3.1 Wavelength-Routed WDM Networks

Although current optical networks provide high bandwidth, they suffer from the electronic bottleneck, which happens in the network node for O-E-O conversion. To eliminate the electronic bottleneck, the next generation of optical networks will be capable of selectively routing and switching individual wavelengths, creating what is called a wavelength-routed optical WDM network. In doing so optical technology can be used at a truly network level, instead of remaining a link level technology. In a wavelength-routed optical WDM network, each wavelength can be routed through the optical network at the optical switching nodes, removing the need for opto-electronic conversion and electronic routing. Data can remain in optical domain without requiring costly high-speed electronic equipment and eliminate the bottleneck due to O-E-O conversion at intermediate router nodes. Critical pieces in enabling the deployment of wavelength-routed optical WDM networks are the intelligent optical components, such as optical crossconnects (OXC), wavelength add-drop multiplexers (WADM), and a feasible and effective control plane for WDM networks. The control plane of wavelength-routed optical networks is responsible for control and management of the optical networks, including configuration management, fault management and performance management. In this chapter, we mainly focus on connection management,

which is one of the critical functionalities of configuration management. Provisioning of connections, in a wavelength routed WDM network, requires algorithms for route selection, and signaling mechanisms for requesting and establishing connectivity. An effective and feasible connection management method for WDM networks is based on a suitable network control scheme and RWA (routing and wavelength assignment) scheme. In the following sections, we will discuss connection management in more detail and compare different methods for implementing connection management through the control plane in optical networks.

3.2 Connection Management

Connection management of optical networks can be implemented using different strategies. In this section, we compare the different connection methods from different points of view, using the critical metrics for connection management, such as blocking probability, connection setup time, network resource utilization, network resource cost etc. Connection management schemes can be classified using several criteria. From the system architecture point of view, we can distinguish between centralized or distributed methods that require different amounts of network resource knowledge. Based on the holding times of the lightpaths, there are static and dynamic connection management methods. Depending on the network requirements, network design engineers can choose different signaling methods: in-band or out-of-band.

3.2.1 Centralized and Distributed Approaches

Two kinds of connection management methods, Centralized and Distributed, can be employed in optical networks. In the centralized one, a central control center/central network management system for the whole network holds the global information of the network, such as the network topology, the link states, the wavelength usage on each link and the status of each network element. When a source node needs to transfer data, the request for connection is sent to the control center and then a route is calculated, according to the routing and wavelength assignment algorithm in the center, based on the global information of currently available network resources. Then, the control center will reserve the resources for the connection by notifying each node along the route. After the control center receives acknowledgment from each node, it will send a

message to notify the source node to send data along with the reserved path to the destination. When a connection is finished, the control center will signal each node involved to release the selected wavelength.

In the distributed approach, each node along the route will be involved in making decisions on selecting the wavelength. The connection request goes through each node along the route and reserves the wavelengths based on the local information (or partial information of the network) at the node. After all the nodes on the route agree to the request, the source will start sending data along the reserved route. When a connection is torn down, the release request will be sent to the destination and release network resources being used at each node. A path is decided by coordination among the different nodes, not by a control center. And, the information stored at each node needs to be sent out to other nodes to react to changes in the node status. It is called a distributed approach due to its distributed nature of operation. Because the centralized approach does not need coordination from each node for computing a lightpath, it is simple to a implement and effective in small-sized networks. Another advantage of a centralized approach, over the distributed one, is its lower blocking probability, due to the fact that the central control center knows the updated information of the whole network. But, the centralized method is vulnerable due to the presence of a single point of failure. If the control center crashes, the whole system cannot work properly. Another disadvantage with the centralized approach is its lack of scalability. When the network becomes large, the information needed to be stored at the control center becomes staggeringly large. Consequently, the computation time becomes large and the control center will become the bottleneck for the whole network. Moreover, since different sub-networks may be using equipment from different vendors, sub-networks may have their own control centers, which differ from one other. So if the network becomes large enough to contain many vendors' network elements, interoperability between sub-networks will be a problem.

Compared with the centralized approach, the distributed one is more suitable for a large-scale network. It leaves the decision of selecting the local wavelength to each node and distributes the computation task to each node on the route and thus it eliminates the bottleneck due to the control center and improves the reliability of the network. Different vendors' network elements can communicate with one other using well-

known routing protocols and wavelength assignment protocols. So it also provides better scalability. But, the distributed approach increases network resource costs, because it requires changing the state of each node in the network and increases the complexity of the system. It also has a higher blocking probability than the centralized one, due to its distributed working fashion.

3.2.2 In-Band and Out-Band Signaling

A standard signaling system needs to be set up for conveying connection related information in optical networks. The availability of the signaling channel, which transports signaling messages, is of crucial importance in an optical network. The channel can be either in-band or out-of-band. For in-band signaling, the signaling messages are carried on the same channel as the data, maybe using the overhead frames in the data channels. For example, the Synchronous Optical Network (SONET) overhead frames can be used to carry signaling messages. However, all optical networks do not extract the content of signaling messages at the intermediate switching nodes and cannot implement O-E conversion to process the signaling messages. So it is impractical to implement in-band signaling for all optical networks, although it could enhance the network resource utilization by making use of the overhead bytes. Out-of-band signaling employs a separate network for signaling message transportation. It can obtain high-speed signaling for large volume of information at the expense of consuming more networking resources.

3.2.3 Path Multiplexing and Link Multiplexing

In dynamic wavelength routing networks, a link refers to a link/wavelength between two adjacent optical switching nodes. A lightpath refers to the optical path (route), and one/several chosen wavelengths from a source station to a destination station through intermediate optical switching nodes (OXC). We can regard a lightpath as a virtual pipe-line for transferring data across a WDM network. When the same wavelength is used on each link along the lightpath, it is called PM (path multiplexing). When different wavelengths (or possibly the same one) are used in each link along the lightpath, it is called LM (linkmultiplexing). The additional condition required in PM is referred to as the wavelength continuity constraint. The bandwidth usage of PM is lower

than that of LM. The restriction imposed by the wavelength continuity constraint can be avoided by the deployment of wavelength converters at each wavelength routing node.

3.2.4 Different RWA algorithms for PM

A good wavelength assignment algorithm in a PM network can result in improved performance. Here, we list some proposed wavelength-assignment algorithms:

Random wavelength assignment: Selecting wavelengths randomly from a set of available wavelengths.

First-fit wavelength assignment [11]: Selecting the first available wave-length according to a predefined order of wavelengths.

Most-used wavelength assignment [12]: Selecting the wavelength, which is used most in the available wavelength pool.

Least-used wavelength assignment [12]: Selecting the wavelength, which is used least in the available wavelength pool.

Karasan and Ayanoglu [14] used network simulations to investigate the performance of the least-used, randomly selected, most-used, and first-fit wavelength assignment algorithms in networks with a single fiber on each link. Shortest path routing was used as the routing method. The blocking probability and networking utilization were used as the evaluation standard.

They showed through experiments that the least-used heuristic provides the worst performance. The performance of random wavelength assignment was found to be slightly better than the least-used one, since it effectively balances the traffic load on each wavelength. They showed that the most-used wavelength algorithm, especially in networks with large number of wavelengths, could improve the network performance. But, the algorithm needs a global knowledge of the network status. First fit wavelength assignment can achieve a good performance almost close to the most-used wavelength assignment algorithm. The benefit of the first-fit algorithm is that it only needs the state

of the links along the lightpath, instead of global knowledge of network status as required by the most-used wavelength algorithm.

3.2.5 Static and Dynamic Assignment

In static WDM networks, lightpaths are assigned in advance and remain unchanged for a long period, perhaps several days. So the connection from one node to another node is fixed on some lightpaths during that period. If the bandwidth requirement of the traffic and the statistical properties of the traffic can be known in advance and remains unchanged for a long term, static WDM networks can work well. Although static WDM networks are not as complex as the dynamic one and reduce the processing time for computing lighpaths, the network bandwidth utilization is low under static connection configuration. Dynamic configuration requires that lightpaths are established on demand. Each time, when a node needs to send data, it will request a lightpath from the network. The lightpath, route and wavelengths, is calculated for each request. In a realistic network, lightpaths may be designed under a combination of both static and dynamic configurations, in order to obtain a more effective performance.

3.2.6 Source Initiated Reservation and Destination Initiated Reservation

In a Source Initiated Reservation (SIR) approach, wavelengths are reserved along the way when the connection request is sent from the source node to the destination node. In the DIR method, wavelengths are not reserved until the ACK of the connection request is sent back from destination node to source node.

For SIR, the network bandwidth, in terms of reserved wavelengths, is wasted during the reservation period. Using DIR can thus improve bandwidth efficiency. DIR brings obvious benefits for PM, since the request message gathers all the wavelengths usage on the way to the destination and then lets the destination select a wavelength based on the whole wavelength information on each node along the route. LM can also benefit from this approach. If one of the lightpath assignments fails, the destination can select another lightpath based on the gathered information. It reduces the processing time. However, DIR enhances the blocking probability, since it increases the chance of having inconsistent knowledge of wavelength usage at each destination node.

3.2.7 Dropping and Holding Schemes

In the dropping scheme, when the reservation fails at the intermediate node, NACK will be sent back to the source node and the request will be re-sent after a timeout. In the holding scheme, the intermediate node will not send NACK, instead it will buffer the request message and wait for wavelengths to become available at an intermediate node for a specified time interval. The holding scheme reduces processing time and propagation due to lower overhead for resending reservation requests.

3.2.8 Parallel and Sequential Reservation

Sequential reservation selects only one wavelength at each intermediate node. In a parallel method, the source node reserves all the available wavelengths and each intermediate node reserves the available sub-set of the reserved wavelengths. At the destination, a wavelength will be assigned and ACK will be sent back. The ACK is responsible for reserving that wavelength and releasing all the other wavelengths reserved previously. Parallel reservation makes sense only in PM because in LM, any available wavelength could be selected at each link.

3.3 Classification of Routing and Wavelength Assignment Schemes

In what follows, a light-path is defined as an end-to-end connection request between two end nodes, which may span multiple links. A route is a selected path along the multiple optical fibers, which may be located far from each other in the physical network topology. A wavelength is a circuit-switched path for the route, that constitutes an interconnected routing path between two nodes. A message can be sent from one node to another using a specific wavelength, without requiring any buffering and electro-optical conversion at the intermediate nodes.

Basically, a RWA problem can be formulated as follows. Given a set of light-paths that need to be established on the network, and given a constraint on the number of wavelengths, we need to determine the routes and the wavelengths that should be assigned to the light-paths so that the maximum number of light-paths may be established (or the minimum number of required wavelengths used or the minimum light-path blocking probability is achieved). The routing problem is solved by

techniques based on the shortest path algorithm. The wavelength assignment problem is solved by graph coloring techniques for the selected routes. Hence, the RWA problem can be defined as an optimization problem in a number of ways using various cost functions. Figure 3-1 shows a functional classification of RWA problems. The RWA problem is partitioned into two sub-problems; routing and wavelength assignment.

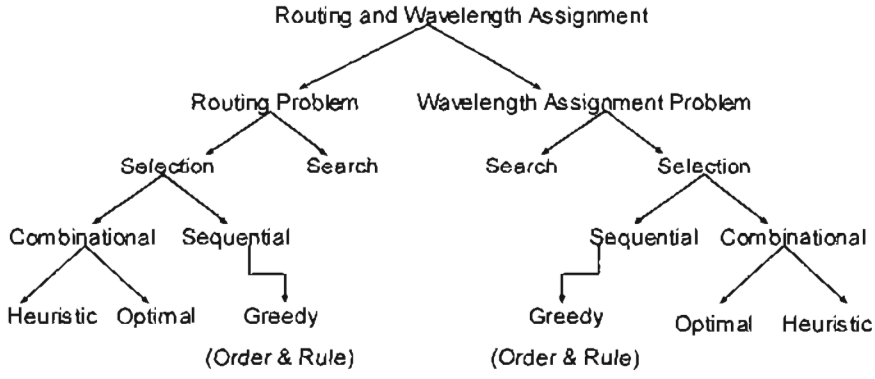


Figure 3-1 Functional Classification of routing and wavelength assignment algorithms

We can further divide each routing and wavelength assignment problem into two components (1) search and (2) selection functions. Figure 3-2 and Figure 3-3 give example algorithms for solving each functional element described in the routing and wavelength assignment problems, respectively.

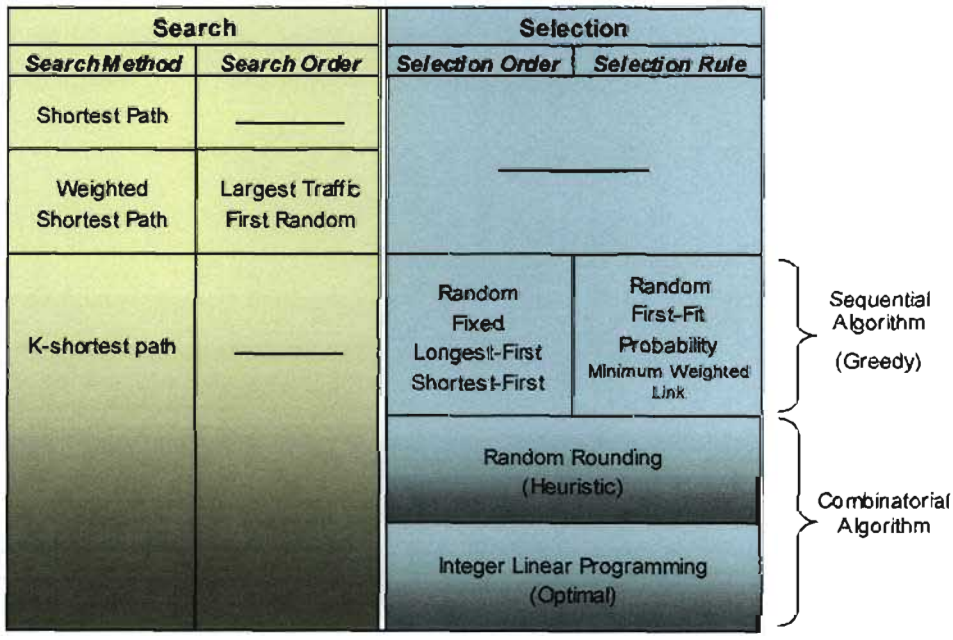


Figure 3-2 Functional elements of routing algorithm

3.4 Functional Elements of Routing Algorithms

In routing problems, taking into account all possible source and destination pairs is impractical because the number of state space is exponentially increased with the number of network nodes and links. Hence, the search function is usually performed by well-known techniques such as shortest-path algorithm and its variations. In k-shortest path algorithm (i.e., more than one route is available), the selection function is performed by either sequential or combinatorial optimization algorithms. Sequential algorithm (called greedy algorithm) is the simplest one in that the selection for each light-path is done sequentially. This technique does not change the results of the previous one, but it consider the results of the previous one. It requires two sub-functions; the selection order and the selection rule. The selection order is the selection sequence of light-paths to be routed (or to be assigned). The selection rule is a decision criterion to choose one of the available candidates. On the other hand, combinatorial selection techniques consider the inter-dependency of light-path routing. The combinatorial methods are divided into two approaches; optimal and heuristic mechanisms. The optimal approaches use all possible combinations of the inter-dependency. Heuristic methods reduce the combination space. The optimal selection achieves the best result, but, the cost of computational complexity becomes critical. Figure 3-2 illustrates functional elements for routing algorithm. The description of each function is as follows

Shortest path (SP): Shortest path algorithms find the shortest route from a given source to a destination in a graph. The route is a path whose cost is less than any other route from the source to the destination. The cost function is often the sum of weights of the edges on the path. Typically, the weights on the graph are static and independent of the number of routes on the link. The shortest path algorithm generates one route and it is independent of other selections. Hence, SP does not require any search order/rule or selection functions.

Weighted shortest path (WSP): Weighted shortest path algorithms are a shortest path algorithm, but the link cost may be dynamically changed depending on the number of routes established. Hence, it requires a search order. Some examples are as follows:

- Largest traffic first schemes line up the light-paths to be routed starting the light-path with the largest traffic first in an attempt to search a route.

- Random schemes lines up the light-paths to be routed in random order.

However, this does not require any selection function since it also finds one route for each source and destination pair.

k-shortest path: k-shortest path algorithms find more than one route for each source and destination pair. k alternative paths provide the flexibility in route selection. However, the routing problem is transformed into a selection problem, where routes are selected to obtain a minimum cost (total number of hop or link cost) for all source and destination pairs.

The selection functions are as follows:

Sequential selection (Greedy algorithm)

Selection order

- Random schemes line up the light-paths to be routed in a random order in attempt to select routes.
- Fixed schemes line up the light-paths to be routed in a given order (e.g., alphabetical order).
- Longest-first schemes line up the light-paths to be routed as the longest (hop or cost) path first.
- Shortest-first schemes line up the light-paths to be routed as the shortest (hop or cost) path first.

Selection rule

- Random schemes randomly choose one route among candidates.
- First-fit schemes choose the first matched one route among candidates.
- Probability schemes choose one route among candidates with probability.
- Minimum-weighted link first schemes choose the route on the link that includes minimum number of established routes.

Combinatorial selection

- For an optimal solution, a mixed integer program is used, which is modeled with the multi-commodity flow problem. This is extremely difficult in terms of computational complexity.
- For a heuristic solution, a random rounding algorithm is proposed. In this approach, routing algorithm is repeatedly performed for different set of routes

while the maximum number of links in all routes is decreased through an alternative selection of routes. The process is repeated until no further improvements are possible.

3.5 Functional Elements of Wavelength Assignment Algorithms

As shown in Figure 3-3 the wavelength assignment problem can also be defined in terms of search and selection.

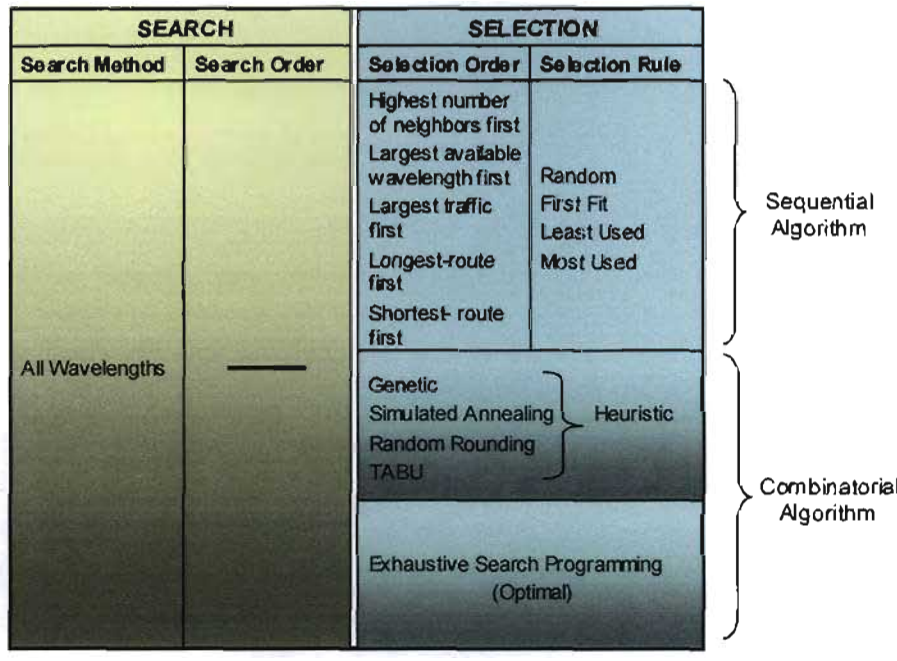


Figure 3-3 Functional elements of wavelength assignment algorithms

The search is simple since any available wavelength can be assigned along the selected route. The remaining problem is the selection among available wavelengths, which can maximize the wavelength utilization. Selection is further classified into sequential and combinatorial approaches similar to that of routing algorithms.

The sequential approach sorts routes to be assigned. Then, a wavelength is assigned to the sorted routes. On the other hand, combinatorial selection considers inter-dependency of each selection. It is further broken into optimal and heuristic approaches. The optimal approach is a well-known NP-complete problem which is difficult to apply to large networks. So, heuristic approaches are hard to reduce the search space to a

smaller set of light-paths, although they may increase the number of wavelengths. A number of heuristic methods have been proposed. They are based on well-known graph coloring methods such as meta-heuristic mechanisms. The descriptions of each functional element are as follows:

Sequential selection (Greedy algorithm)

Selection order

- Largest number of neighbor-first schemes sorts the routes according to the number of neighbors at an attempt to assign an available wavelength.
- Largest available wavelength-first schemes sort the routes in the order of available wavelengths.
- Largest traffic -first schemes sort the routes in order of traffic requirement.
- Longest path-first schemes sort routes in order of the number of hop counts for each route.
- Shortest first schemes sort the routes with the shortest number of hop first.
- Random schemes sort routes in a random order.

Selection rule

- First fit schemes attempt to select the first available wavelength in numerical order.
- Most used schemes attempt to allocate the most utilized wavelength first.
- Least used schemes attempt to allocate the least utilized wavelength first.
- Random schemes attempt to allocate a wavelength randomly.

Combinatorial selection

- Optimal selections can be solved by exhaustive search. Exhaustive search algorithms always generate the best coloring result for a given graph. But, they do not ensure that the algorithm can handle considerably large graphs, too.

- Heuristic selection algorithms work very well with graph coloring problems that are further divided into;

- Genetic algorithms (GA) are standard techniques for hard combinatorial optimization problem. The basic idea is to simulate evolution of genotypes and natural selection, which has been applied to global optimization especially combinatorial optimization problems. The idea is based on the specification of three operations (each one is probabilistic) on objects called strings;

    1. Reproduction-combining strings in the population to create a new string (offspring),
    2. Mutation-spontaneous alteration of characters in a string, and
    3. Crossover-combining strings to exchange values, and creating new strings in their place. The reproduction and crossover operations can include competition within populations.

- Simulated annealing algorithms (SA) are another standard techniques for hard combinatorial optimization problem. The idea is to simulate annealing of some object in order to overcome a local minimum point in a sense of iterative improvement. Basically, it is based on the metaphor of how annealing works: reaches a minimum energy state upon cooling a substance, that is, it allows a non-improving move to a neighbor with a probability that decreases over time.

- TABU algorithms are relatively new heuristic methods. The basic idea is a random local search, but some movements are forbidden. This should make it possible to get away from local minima.

A detailed explanation of the manner in which wavelength routing and connection management is carried out in DWDM networks has been presented in the preceding sections. In sections that will follow, the objective is to provide reasons to substantiate the choice of one wavelength assignment scheme or routing algorithm over another, in addition to this the overflow model is discussed briefly.

3.6 Wavelength Conversion Gain

In WDM networks it is desired that a wavelength can be routed without electrical conversions. Two technologies are possible for this purpose: wavelength selective cross-connects (WSXC) and wavelength interchanging cross-connects (WIXC), which

involve wavelength conversion. Two metrics can be used to quantify the wavelength conversion gain:

- The reduction in blocking probability gain and
- The increase in maximum utilization gain, compared to a network without converters.

The overflow model is used to analyze the blocking probability for wavelength-selective (WS) networks using the first-fit wavelength assignment algorithm.

In a WS network a connection can only be established if the same wavelength is available on all links between the origin and the destination nodes. This means that a connection request can be blocked even if there are available wavelengths on all links. The blocking probability can be reduced by allowing the connection to change from one wavelength to another at an intermediate cross connect, which is known as wavelength conversion. A network in which all cross connects have wavelength conversion capability (from any wavelength to any other wavelength) is called a wavelength-interchangeable (WI) network. The utilization gain G_u is defined as the ratio of maximum offered loads for WI and WS for achieving a given blocking probability [13]. Similarly the blocking probability gain G_p is defined as a ratio of blocking probabilities for WS and WI networks for a given traffic load as shown in Figure 3-4.

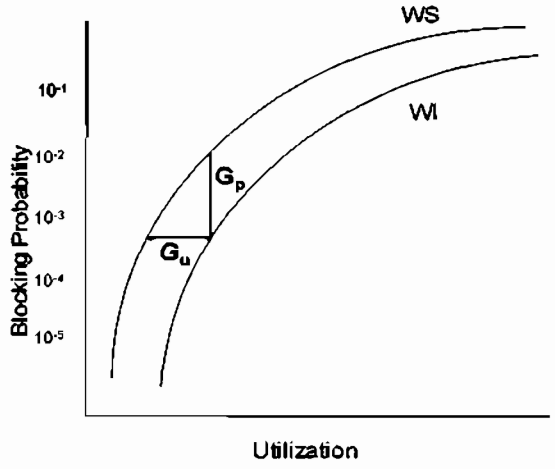


Figure 3-4 Blocking Probability versus Utilization

In the literature most analytical studies for obtaining the blocking probability P_b for WS networks assume that all wavelengths have identical traffic loads, this is only the case for some wavelength selection algorithms such as random selection rule[14]. With the first fit rule the traffic load on each wavelength decreases as the wavelength number increases. The literature [15] [16] proposes the use of the overflow model to calculate the blocking probability P_b with the first fit algorithm, since this model performs well when analyzing circuit switched networks with non-Poisson traffic.

3.7 The Overflow Model

In the overflow model it is assumed that all traffic is offered to the first wavelength and the overflow traffic from wavelength k is offered to wavelength $k+1$. The traffic overflowing from the last wavelength is the blocked traffic. The second moment of the overflow traffic is used in computing the blocking probability for each wavelength. The numerical studies presented in the literature using the overflow model show a close match between the analytical and simulation results. The model presented in [13] and developed later in [11] and [17] provides equations which can be used to study the qualitative behavior of the utilization gain G_u^p for path p as a function of the path length, number of wavelengths, and number of fibers when the random wavelength selection algorithm is used. The utilization gain is upper bounded as

$$G_u^p \le \left(\frac{H_p}{L_p}\right)^{\frac{1}{M}} \qquad 3.7.1$$

where H_p is the number of links on path p, L_p is the average number of links shared by paths intersecting with p (*interference length*), and M is the number of fibers per link. An approximation for G_u^p as $P_b \to 0$ is obtained as

$$\lim_{P_b \to 0} G_u^p = \left(\frac{H_p^{1-\left(\frac{1}{K}\right)}}{L_p}\right) \qquad 3.7.2$$

where K is the number of wavelengths per fiber [19].

The effect of the topology and the routing algorithm on can be studied using (3.7.1) and (3.7.2). As the network gets larger, i.e., larger average path length H, G_u increases. More importantly, shortest path routing which minimizes H for a given network reduces G_u. We observe from (3.7.2) that as the average interference length L gets larger, G_u decreases. The interference length not only depends on topology but also is determined by the routing algorithm. Shortest path algorithms such as Dijkstra or Bellman-Ford [20] produce paths sharing multiple links (large L). On the other hand, routing algorithms which use a larger number of paths per node pair (such as k shortest paths) produce smaller L.

The effect of K, the number of wavelengths, is weak as $P_b \to 0$, much weaker than M, which reduces G_u exponentially. The strong dependence on M is significant since with the current WDM technologies there are technological and economical advantages of having multiple fibers on each optical link.

3.7.1 Analysis of Blocking Probability using the Overflow Model

Traffic offered to wavelength 1 for any path p is equal to the total traffic offered to path p. We assume that connection requests arrive to a node according to a Poisson process with rate λ with uniformly selected destinations and exponentially distributed holding times with mean $1/\mu$. We also assume that a single path is used for each source-destination pair. The traffic offered to wavelength 1 for any path p is given by

$$A_1^p = \frac{\lambda}{\mu(N-1)} \qquad 3.7.1.1$$

where N is the number of nodes in the network. Although the offered traffic for wavelength 1 is Poisson, the overflow traffic from each wavelength is bursty. Therefore, the assumption that the traffic offered to each link for any wavelength is Poisson underestimates the link blocking probability. Instead, we apply the equivalent random

method [15], [21] which uses both the mean A_{lk} and the variance V_{lk} of the bursty traffic offered to link l for wavelength k, $k \geq 2$ to obtain the link blocking probability B_{lk}.

The variance V of the overflow traffic from a system of M channels with Poisson-offered traffic is given by the Brockmeyer model [15]

$$V = \vartheta\left(1-\vartheta+\frac{A}{M+1-A+\vartheta}\right) \qquad 3.7.1.2$$

where A is the mean offered traffic and ϑ is the mean overflow traffic. Mean overflow traffic is given by $\vartheta = AE(A,M)$, where $E(A,M)$ is the Erlang-B formula. The number of channels M in (3.7.2.2) corresponds to the number of fibers per link since the number of channels for each wavelength on a link is given by the number of fibers on that link. In the overflow model the offered traffic for wavelength $k+1$ on path p is given by the overflow from wavelength k on p

$$A_{k+1}^{p} = \vartheta_{k}^{p} = A_{k}^{p} B_{k}^{p} \qquad 3.7.1.3$$

where B_k^p denotes the blocking probability on path p for wavelength k. We assume that for a given path p and wavelength k the events corresponding to blocking of wavelength k on each link along p are all independent, i.e.

$$B_{k}^{p} = 1-\prod_{l\in p}(1-B_{lk}) \qquad 3.7.1.4$$

where B_{lk} is the blocking probability on link l for wavelength k.

A connection request that arrives on a link and finds a free wavelength does not immediately produce a new call in service. If this wavelength is not available on the rest of the path, this connection request cannot be established. Hence, the traffic offered to a link depends on the blocking probability of links that appear before and after it on a path. Let A_{lk}^{p} denote the offered traffic to link l originating from path p for wavelength k.

A_{lk}^{p} is given by the reduced load model [15], this technique is also called the Erlang fixed-point equation.

$$A_{lk}^{p} = A_{k}^{p} \prod_{l' \in p, l' \neq l} (1 - B_{l'k}) = A_{k}^{p} \left(\frac{1 - B_{k}^{p}}{1 - B_{lk}} \right) \quad \text{, for } l \in p \qquad 3.7.1.5$$

where A_{k}^{p} is the offered traffic to path p for wavelength k.

The total traffic A_{lk} offered to link l for wavelength k is given by the sum of the offered loads for the paths passing through l

$$A_{lk} = \sum_{p, l \in p} A_{lk}^{p} \qquad 3.7.1.6$$

The link blocking probability B_{lk} for wavelength k resulting from the reduced link load A_{lk} given by (3.7.1.6) is found by using the equivalent random method and the Brockmeyer model given by (3.7.1.2). Let V_{lk} denote the variance of the traffic offered to link l for wavelength k. Since the traffic offered for wavelength 1 is Poisson, its mean is equal to its variance, i.e., $V_{l1} = A_{l1}$ for all links. The mean ϑ_{lk} and variance $\hat{V}_{lk}$ of the overflow traffic from wavelength k for link l are given by

$$\vartheta_{lk} = A_{lk}^{*} E(A_{lk}^{*}, M_{l} + M_{lk}^{*}) \qquad 3.7.1.7$$

and

$$\hat{V}_{lk} = \vartheta_{lk} \left(1 - \vartheta_{lk} + \frac{A_{lk}^{*}}{M_{l} + M_{lk}^{*} + 1 - A_{lk}^{*} + \vartheta_{lk}} \right) \qquad 3.7.1.8$$

The variance of the overflow traffic from wavelength k is equal to the variance of the offered traffic for wavelength $k+1$, i.e.

$$V_{l,k+1} = \hat{V}_{lk} \qquad 3.7.1.9$$

The parameters A_{lk}^{*} and M_{lk}^{*} in (3.7.1.7) and (3.7.1.8) are the equivalent Poisson traffic load and the equivalent number of fibers, respectively, which are given by the solution to the equations

$$A_{lk} = A_{lk}^{*} E(A_{lk}^{*}, M_{lk}^{*}) \qquad 3.7.1.10$$

and

$$V_{lk} = A_{lk}\left(1 - A_{lk} + \frac{A_{lk}^{*}}{M_{lk}^{*} + 1 + A_{lk} - A_{lk}^{*}}\right) \qquad 3.7.1.11$$

The solutions A_{lk}^{*} and M_{lk}^{*} to (3.7.1.10) and (3.7.1.11) are obtained iteratively, and the link blocking probability B_{lk} is given by

$$B_{lk} = E(A_{lk}^{*}, M_l + M_{lk}^{*}) \qquad 3.7.1.12$$

Note that the parameter M_{lk}^{*} is, in general, not an integer, and the generalized Erlang-B function is used in (3.7.1.10) and (3.7.1.12) [15]. Given the mean link traffic A_{lk} and variance V_{lk} , the link blocking probabilities are computed using (3.7.1.10)-(3.7.1.12), and these blocking probabilities are used to obtain the mean link traffic A_{lk} by using (3.7.1.5) and (3.7.1.6). This iterative procedure is continued until the link blocking probabilities converge. Once the procedure for wavelength k is finished, the mean and the variance of the traffic for wavelength $k+1$ are obtained from (3.7.1.3) and (3.7.1.4), and (3.7.1.7)-(3.7.1.9), respectively.

The algorithm for obtaining the blocking probability with the overflow model is described below in detail.

For $k = 1$:

1.1) compute $\left\{A_1^P\right\}$ from (3.7.1.1);

1.2) assume initial values for link blocking probabilities $\{B_{l1}\}$;

1.3) for each link l, find A_{l1} from (3.1.7.5) and (3.1.7.6);

1.4) for each link l, $V_{l1} = A_{l1}$;

1.5) solve for A_{l1}^* and M_{l1}^* by iterating between (3.7.1.10) and (3.7.1.11);

1.6) compute B_{l1} from (3.7.1.12);

1.7) if B_{l1} values converged, compute $\left\{B_1^p\right\}$ from (3.7.1.4), obtain $\{\vartheta_{l1}\},\{\hat{V}_{l1}\},\{V_{12}\}$, from (3.7.1.7)-(3.7.1.9), and go to $k = 2$; else go to 1.3.

For $1 \le k \le K$:

k.1) compute $\left\{A_k^p\right\}$ from (3.1.7.3);

k.2) assume initial values for link blocking probabilities $\{B_{lk}\}$;

k.3) for each link l , find A_{lk} from (3.1.7.5) and (3.1.7.6);

k.4) solve for A_{lk}^* and M_{lk}^* by iterating between (3.7.1.10) and (3.7.1.11);

k.5) compute $\left\{B_{lk}\right\}$ from (3.1.7.12);

k.6) if $\left\{B_{lk}\right\}$ values converged, compute $\left\{B_k^p\right\}$ from (3.1.7.4),obtain $\{\vartheta_{lk}\},\{\hat{V}_{lk}\},\left\{V_{l,k+1}\right\}$ from (3.1.7.7)–(3.1.7.9), and go to $k+1$; else go to k.3.

Once $\left\{B_k^p, k = 1,...K\right\}$ are computed, the connection blocking probability is readily calculated. A connection request is rejected when it is not possible to establish it on any wavelength, and the mean connection blocking probability is given by

$$P_b = \frac{\sum_p A_1^p \prod_{k=1}^{K} B_k^p}{\sum_p A_1^p} \qquad 3.7.1.13$$

The overflow model is more accurate for fairly connected topologies for which the link independence assumption (3.7.1.4) is applicable. The accuracy of the model decreases as the number of wavelengths increases because of the successive application of the equivalent random approximation.

3.7.2 Conclusions from Previous Works

From the literature, simulations to compare blocking probabilities of various wavelength assignment algorithms were carried out on networks using either a single fiber or multi fiber links. In most experiments wavelengths were selected in accordance with Multiwavelength Optical Networking (MONET) Architecture [22]. In the case of multifiber network, network designs were carried out using traffic demand matrix $T = \left[t_{ij} \right]$, where t_{ij} is the number of wavelength demands between nodes i and j. The traffic matrix T does not represent the actual traffic but rather the forecasted traffic that will be carried by the designed network. The number of fibers for each link was chosen by routing each traffic demand along the shortest path. Key areas of interest were the performance of wavelength assignment algorithms for the WS network as compared to the performance of the WI network which has the same number of fibers per link as WS network. From experiments conducted in the literature, the blocking probability is evaluated for the single-fiber case as a function of the traffic load. The load was expressed by the link utilization per wavelength given by

$$\rho = \frac{N\lambda H}{JMK} \qquad 3.7.2.1$$

Where N is the number of nodes, H is the average number of links per path, J is the number of links, and M is the average number of fibers per link.

When the network has multiple fiber links, the usage level at each wavelength can be used to determine the link load, for the multifiber case, algorithms that choose the wavelength based on the load values along the shortest path were used. Two such algorithms are the Least Loaded (LL) and Minimum Sum (MS) algorithms.

Let M_l denote the number of fibers on link l and let A_{lj} denote the number of fibers (or optical connections) for which wavelength j is utilized on link l. The set of available wavelengths along the shortest path p is denoted by S_p. The following two dynamic wavelength selection algorithms for the multiple-fiber case were found to be used.

• *Least-loaded (LL)*: The minimum index wavelength j in S_p that achieves

$$\max_{j \in S_p} \min_{l \in p} \left[M_l - A_{lj} \right] \qquad 3.7.2.2$$

is selected.

• *Minimum sum (MS)*: The minimum index wavelength j in S_p that achieves

$$\min_{j \in S_p} \sum_{l \in p} \frac{A_{lj}}{M_l} \qquad 3.7.2.3$$

is selected.

The LL rule selects the wavelength that has the largest residual capacity on the most loaded link along. The MS algorithm chooses the wavelength that has the minimum average utilization.

It was found that the first-fit algorithm performs much better than the random algorithm at low loads, whereas the difference between the two algorithms is marginal at higher utilizations. The most-used algorithm offers slightly better performance than the first-fit algorithm. Most of call blockings occur at lower utilizations due to wavelength conflicts hence the selection algorithm plays an important role in the low blocking probability region.

Experiments were also conducted for the multiple-fiber network with different wavelength selection algorithms. Both adaptive wavelength selection algorithms perform much better than the random, first-fit and most-used selection rules. The order of performance between the random, first-fit, and most-used algorithms is the same as the single-fiber case; however, the performance differences between these algorithms are much smaller. Among the two adaptive wavelength selection rules, the MS is slightly better, especially at lower utilizations. The wavelength conversion gain for the multifiber case was found to be significantly less than the single-fiber case, as predicted by [17] and [19].

After comparing the various algorithms, the wavelength packing type algorithms such as the first fit rule perform better than the random rule, especially when number of fibers per a link is small. Efficient utilization of wavelengths in DWDM networks is one of the key contributors to ensuring network survivability. The overflow model is one of the tools that can be used to accurately obtain the blocking probability which in turn can be used to calculate the blocking probability gain. This together with utilization gain is used as the two metrics to quantify the wavelength conversion gain which is used to judge the most suitable wavelength assignment algorithm.

Chapter 4

Survivability Strategies in Optical Networks

A brief description of existing strategies for protection switching is presented in this chapter, thereafter the chapter focuses on survivability of WDM ring networks, with respect to optimum utilization of spare components. Failure classification is then discussed. The aim of this chapter is to present the various protection mechanisms that attempt to improve the overall efficiency of link restoration in optical WDM networks.

4.1 Survivability in Conventional Transport Network

The issue of survivability arose in telecommunications long before the introduction of the WDM layer. Thus the main electronic layers of the transport network have well known protection mechanisms in place. An example of this is the recovery techniques for a circuit and packet switching environment have been defined for SDH/SONET and IP respectively. The former are based on automatic IP routing table reconfiguration or on flexible load sharing mechanisms. These two functions are supported by all the main IP routing protocols such as OSPF (open shortest path first), BGP (border gateway protocol).

The goal is to have direct implementation of IP over WDM and in most transport networks at present SDH/SONET layer is client to the WDM layer. As a result before WDM protection was defined, SDH/SONET protection mechanisms were mainly adopted to guarantee optical network survivability.

Since we have such effective protection standards in the electronic layers, it may seem redundant to try and incorporate further protection functions in the WDM layer. However there is a very valid motivation for this, the main reason is to exploit the optical layer to reduce fault recovery time. SDH protection schemes have typical recovery times of 60 to 100 ms. Another justification is that failures should generally be solved in the layer in which they occur. Managing optical protection at a low protocol layer, just above the physical layer implies that the control plane has direct knowledge

of the physical topology and behaviour of the network. Information regarding optical circuit performance such as bit error rate, wavelength value etc need not be mediated through many layers. A direct result of this is that the total bandwidth consumed by network control system overhead is reduced and data signalling formats are simplified. These benefits contribute to the increase speed and effectiveness of protection procedures.

4.2 Conventional Network Protection Schemes

Automatic protection Switching (APS) schemes provide a means of recovery from single transmission system failure. The main draw back of this type of switching is that if a composite cable carrying multiple transmission systems is ruptured, normal APS methods will not work since working and protection cables will be broken. The solution to this problem is to diversely route protection cables. Two forms of protection switching are illustrated in Figure 4-1 and Figure 4-2. Figure 4-1 depicts a 1:N APS architecture, this means one protection cable is shared by N working systems and Figure 4-2 shows 1:1 diverse protection architecture with each working cable protected by diversely routed redundant cable.

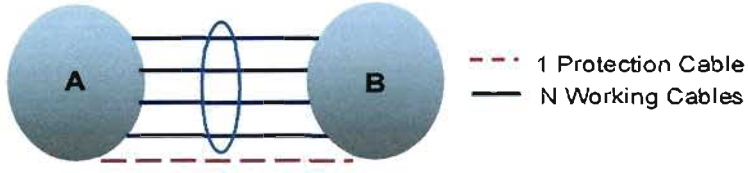


Figure 4-1 1 : *n* Automatic Protection Switching Architecture

Each of these schemes presents a very basic form of protection but it is illustrative of how conventional protection schemes are implemented. The key issue surrounding conventional schemes is that of protection and restoration. Currently the trend is to implement protection and restoration in an optimum manner. The network designer is faced with the task of maintaining an acceptable level of survivability in a most cost effective manner.

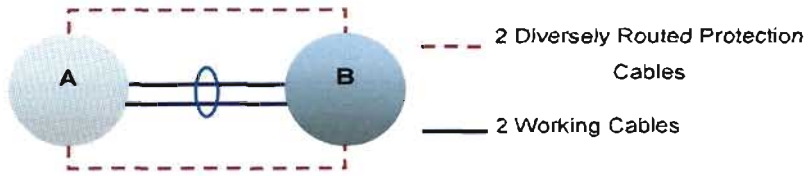


Figure 4-2 1:1 Diverse Protection scheme

Another APS solution is the self healing ring (SHR). This architecture can be implemented in the local loop with add drop multiplexers (ADMs), which serve remote terminals configured in ring topology. The advantage of this type of architecture is that it is resilient since a complete cable cut, severing all contained transmission links, will not isolate a node. In the event of a cable cut, transmission from one node to another adjacent one is still possible over the surviving arc of the ring. Hence recovery from total cable cuts is achieved without the extra cost associated with maintenance of a diverse route as shown in Figure 4-2.

The self-healing ring can generally be divided into two categories: bidirectional SHR's (B-SHR's) and unidirectional SHR's (U-SHR's). The type of ring depends upon the path travelled by a duplex communication channel between each node pairs. The SHR is called a bidirectional SHR (B-SHR) if both directions of a duplex channel travel over the same path; a unidirectional SHR (U-SHR) is classified in this way if the direction of a duplex channel travels over opposite paths.

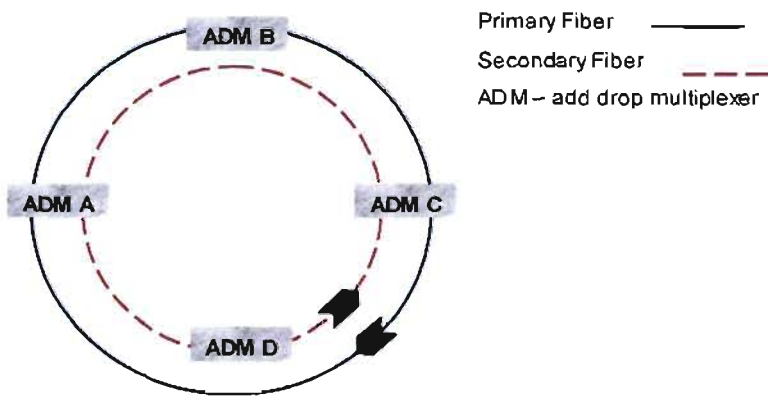


Figure 4-3 Unidirectional self healing ring (U-SHR)

A U-SHR has two fibres referred to as the primary and secondary fibres, these fibres transmit in opposite directions, in Figure 4-3 we consider transmission between A and C. Under normal conditions the communications path from A to C would be ABC, whilst for C to A the path would be CDA, the net transmission is clockwise. Assume a failure occurs between C and D, the ABC channel is unaffected but to switch C to A requires transmission over the secondary path (anticlockwise) be activated. This example shows the protection switching employed by U-SHR.

4.3 Optimization of Spare Components to ensure improved Survivability

Protection Switching is a key technique used to ensure survivability. These protection techniques involve providing some redundant capacity within the network and automatically rerouting traffic around the failure using this redundant capacity.

Redundant components are often used to ensure survivability in a network. However redundancy impacts greatly on the performance and cost implications of the network with obvious tradeoffs. The general idea is to try to achieve as high a level of survivability as possible and at the same time optimize the use of redundant components. Although the U-SHR can be acknowledged as one of the better restoration schemes its main weakness is that it does not perform well for multiple and simultaneous component failures as shown in Figure 4-4

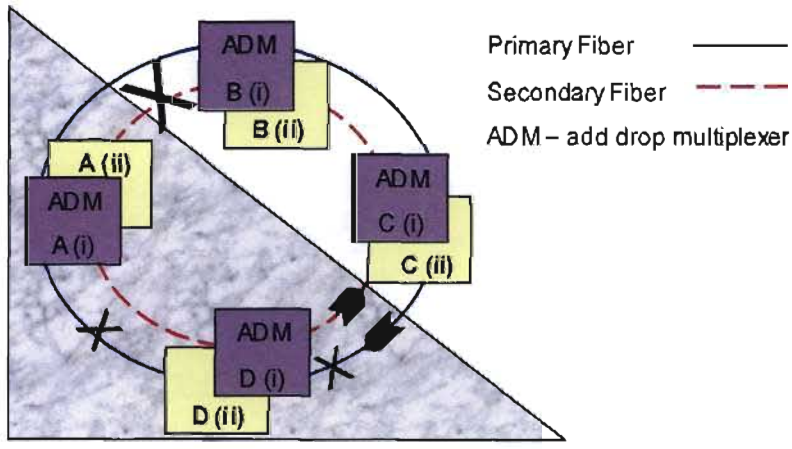


Figure 4-4 U-SHR with multiple faults

The above figure depicts a fully redundant U-SHR with multiple link failures. The shaded region is indicative of high probability of failure. It is apparent that having redundant components is insufficient to sustain survivability, their quantity and location is critical to them fulfilling this role efficiently.

Traffic cannot be recovered using loop back because redundant components are distributed uniformly under the assumption that network components have same failure rate. This assumption may not be true in networks that are deployed in hostile environments where failure rate of equipment could be higher. In order to achieve a reasonably uniform degree of survivability in hostile environments components with high failure rates must have more redundant units than those with lower failure rates. The exact number of redundant units allocated can be obtained using a reliability optimization technique.

Due to the scope of this research we only discuss a model of different failure modes. A few assumptions have to be made as follows; WDM components can fail in one or more modes and each WDM component consists of interconnected parts such as lasers and receivers, each of which fails independently. Two general classes of component failure are being considered, these are the $\alpha - class$ which describes all partial failures and $\beta - class$ which describes total failures. In addition to these classes several modes of failure are defined within the respective classes. All components are subject to α and β classes of failure defined as follows:

α class failures: - Severe class of faults which affects the primary components and redundant units. If one component fails entire subsystem fails.

β class failures: - This class requires all the components in the sub system to fail before the entire subsystem fails.

Each class can contain various modes of failure each with their own failure probability. The logic diagrams in Figure 4-5 define the possible failure modes.

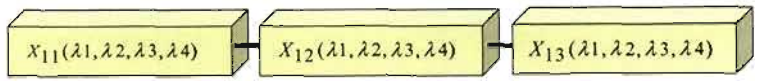


Fig 4-5a α - class failures

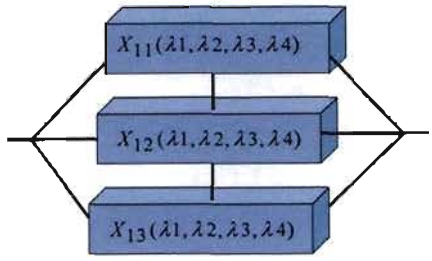


Fig 4-5b β- class failures

Figure 4-5 Logic circuits for different failure classes

Figure 4-5a depicts a logic circuit with series components this models α class failures. The reasoning behind this analogy is that the circuit is considered open if at least one component fails. Similarly the parallel circuit in Figure 4-5b models the β class failures, since the circuit partially functions if one or two components fail. Analysis assumes that the failure probabilities of all components are statistically independent and that redundant units are connected in parallel. The following table is a tabulation of the different classes and their respective modes of failure.

α class failures	
Mode 1	Operational temperature exceeds the set limit
Mode 2	Power failure
β class failures	
Mode 3	Failure of two or three receivers
Mode 4	Failure of two or three transmitters

Table 4-1 Classification of failures

Let p_{ij} be the probability of the i^{th} mode failure in the j^{th} component, where i=1,2 denotes mode of failure in class α and i=3,4 denotes mode of failure in β class. The logic circuits shown in Figure 4-5 are parallel and series configuration of three components interconnected to form a subsystem. The probability that the j^{th} component will fail is given by

$$p_j = \sum_{i=1}^{4} p_{ij} \qquad 4.1$$

Hence, the probability that the subsystem will fail is the sum of the probabilities of its failure in each of the four modes. For the α failures using Figure 3-5b the failure probabilities for modes 1 and 2 are given by

$$q_1 = 1-(1-p_{11})(1-p_{12})(1-p_{13}) \qquad 4.2$$

$$q_2 = 1-(1-p_{21})(1-p_{22})(1-p_{23}) \qquad 4.3$$

For the β class using Figure 3-5a the failure probabilities for modes 3 and 4 are given by

$$q_3 = p_{31}p_{32}p_{33} \qquad 4.4$$

$$q_4 = p_{41}p_{42}p_{43} \qquad 4.5$$

The probability of total failure is the sum of probabilities of failure of each component in each of the four modes of failure.

$$Q = 2-\sum_{i=1}^{2}(1-p_{i1})(1-p_{i2})(1-p_{i3})+\sum_{i=3}^{4} p_{i1}p_{i2}p_{i3} \qquad 4.6$$

This result can easily be extended to a network with m redundant components and s modes of failure, h of which are classified as α failures and the remaining (m-h) are classified as β failures. Using these generalizations the component failure probability becomes

$$Q = h-\sum_{i=1}^{h}\prod_{j=1}^{m+1}(1-p_{ij})+\sum_{i=h+1}^{s}\prod_{j=1}^{m+1} p_{ij} \qquad 4.7$$

If components are alike, the probability of failure given by (5.5) becomes

$$Q = h - \sum_{i=1}^{h} (1 - p_i)^{m+1} + \sum_{i=h+1}^{s} p_i^{m+1} \qquad 4.8$$

where i = 1,2,3....,h denote the α class failures and i = h+1,h+2,h+3,....,s denote the β class failures. Key point to note is that both the working units and the redundant units are subject to the same modes of failure described in Table 1 above.

4.3.1 Problem Formulation

The objective is to optimize the reliability of network components given by (4.7) and (4.8), subject to some design and cost constraints. If the problem objective and cost functions are of the form $W = \sum_{j=1}^{N} f_j(m_j)$ the problem can be classified as separable linear optimization problem with N stages. The stages and redundant units are connected in series. The reliability optimization of a SONET/SDH over WDM ring network can be formulated as an N-stage optimization problem by considering each network component as a stage. For simplicity, we assume that the maximum number of components that can be used in the network at each stage is limited to four. Finding the optimum number of redundant components required to achieve a desired survivability level becomes a constrained reliability optimization problem. Each stage requires a primary component and m_j redundant units. The objective is to determine mj, where $1 \le j \le 4$. The problem is solved using the integer programming approach [5] as follows.

Optimize the following

$$W = \sum_{j=1}^{N} f_j(m_j) \qquad 4.9$$

Subject to

$$\sum_{j=1}^{N} g_{ij}(m_j) \le b_i \qquad i=1,2,3...r \qquad 4.10$$

$$\sum_{j=1}^{M} R_j \ge \ln M \qquad 4.11$$

And

$m_j = 1,2,3,...,\tilde{m}_j \qquad j = 1,2,3,...,N$

where W and m_j are the unknowns

Definition of variables:

N : the number of stages in the system

W : the objective function of the system to be minimized

M : minimum acceptable reliability of the system

m_j : number of redundant units used at stage j

$\tilde{m}_j$: the maximum number of redundant units allowed at stage j

$f_j(m_j)$: the objective function of the i^{th} component as a function of m_j

$g_j(m_j)$: the amount of resources consumed at stage j as a function of m_j

b_i : amount of resources available at the i^{th} stage

r : the number of components

R_j : reliability at the j^{th} stage with $m_j + 1$ (redundant + initial units)

Letting m_j be the number of components used in stage j, the optimization problem can be solved using the integer programming approach presented above.

By using the optimization technique the network resources are used in an efficient way, the redundancy factor can be optimised and hence survivability can be attained in an optimal way.

4.4 Survivability Mechanism Categories

There are numerous mechanisms used in optical networks. They can be classified into three categories namely; shared protection, dedicated protection and restoration

4.4.1 Protection

Protection provides a first level of defence against common faults such as fiber cuts, it is topology and technology specific and offers fast recovery but it may be unable to

protect against node failures or multiple path faults. Protection is typically used in ring networks.

Local defects in network elements are used as triggers, as a result fast detection time can be achieved because physical media faults can be detected within several ms. A fixed amount of capacity is dedicated for protection purposes, this enables fast transfer of traffic from failed facilities to working ones. Depending on how the fixed protection capacity is used, one can differentiate between dedicated and shared protection mechanisms.

4.4.1.1 Dedicated Protection

When this form of protection is applied 50% of the entire capacity in the network is reserved for protection purposes. Dedicated protection delivers the highest level of protection but leads to inefficient network resource utilization. An example of dedicated protection is a Unidirectional Path Switched Ring. This form of protection is often done at layer 1. In linear constellations, providing protection at the optical multiplex section(OMS) layer might be called optical multiplex section protection(O-MSP). In DWDM ring networks, providing protection at the OMS layer is referred to as optical sub network connection protection(O-SNCP). Optical transport networks consist of three layers hence protection can also be supplied at the other two layers. Above the OMS layer, optical channel protection is used at the optical channel layer. Below the OMS layer, line protection is used at the optical transmission section layer.

4.4.1.2 Shared Protection

In shared protection a certain amount of capacity is dedicated for protection purposes and is shared across the resources to be protected. This form of protection is also typically provided at layer 1, in SDH networks, Multiplex section shared protection rings(MS-SPRings) and in SONET networks Bidirectional line-switched rings(BLSR) are used. These mechanisms can also be applied to the OTN, providing shared protection at the OMS layer. Shared protection architectures in the OTN may be called Optical multiplex section shared protection rings (OMS-SPRings) or Optical bidirectional line switched rings(O-BLSR).

4.4.2 Optical Protection ITU-T G.872

The major role of optical protection in multiwavelength networks is to provide reliable point to point connections used to interconnect the service layer nodes. End to end restoration is delivered through service layer restoration. ITU has defined three optical layers in the " Architecture for Optical Transport Networks" in its recommendation G.872, optical protection can be applied at three layers.

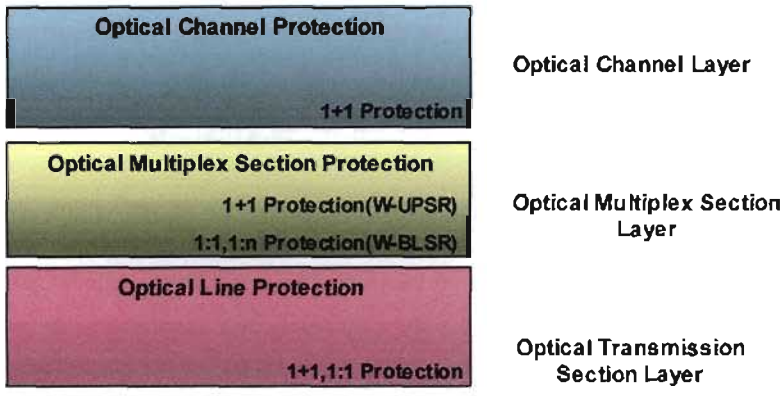


Figure 4-6 Protection in Optical Transport architecture

At the transmission section layer, line protection can be used. At the multiplex section layer, commonly used protection mechanisms of SONET/SDH are applied. At the optical channel layer, optical channel protection is used.

4.4.2.1 Optical Line Protection

Most point to point or ring WDM implementations provide optical layer survivability at the transmission section layer with simple 1+1 or 1:1 line protection, restoring all channels at a time. When using 1+1 protection, the whole DWDM signal is protected by splitting up into two signals in the DWDM node and transmitted over two separate fibres as shown in Figure 4-7. At the receiving node, both signals are compared, and the signal with the better optical signal-to-noise ratio (OSNR) or bit error rate (BER) is chosen.

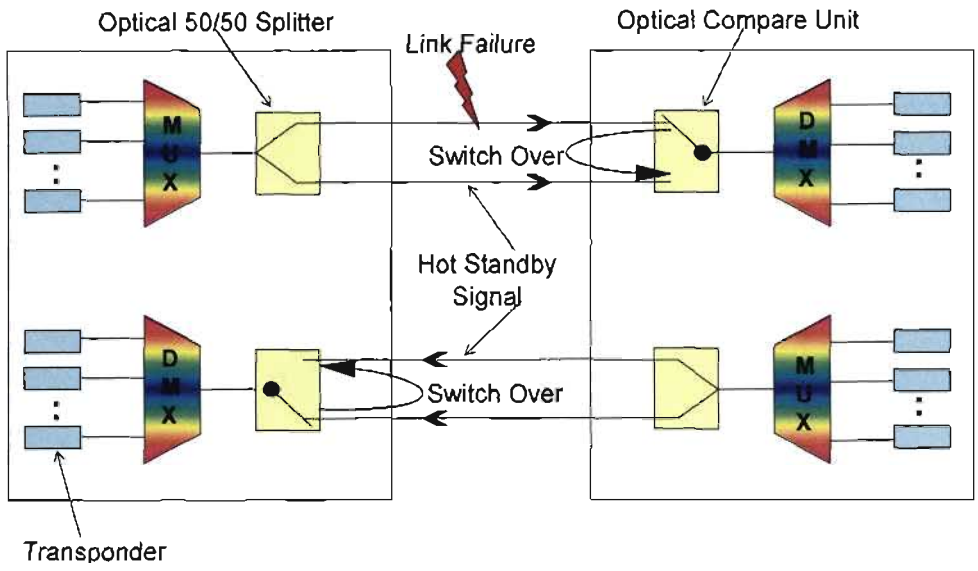


Figure 4-7 Optical 1+1 Protection

When using 1:1 protection, the DWDM signal is sent over only one fiber at a time. If the working fiber fails, the DWDM signal is switched onto the protection fiber as shown in Figure 4-8

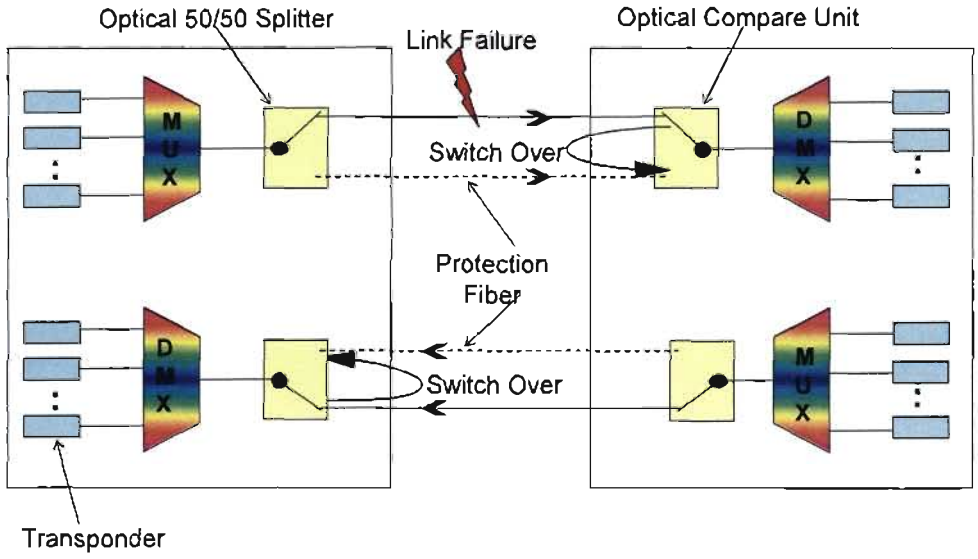


Figure 4-8 Optical 1:1 Protection

With these protection approaches, all optical channels are protected against fiber cuts. The achievable protection time is lower than 10ms.

4.4.2.2 Optical Channel Protection

Using an optical channel protection unit in conjunction with one working and one protection DWDM terminal will provide 1:1 protection for optical channels on a channel-by-channel basis at the optical channel layer.

This protection unit is composed of a transmission section and a receiver section. On the transmission section, the incoming optical client is split by a 50/50 coupler and sent to the transmit transponders of the working terminal and protection terminal as shown in Figure 4-9. On the receiver section, the incoming signals from the receive transponders of the working line and protection line enter in a 1x2 optical switch unit(OSU) that makes the selection in case of failure within the optical layer. The selected channel is then sent to the client receiver. The switching criteria may be based on a signal generated by the receive transponder, due to an input data loss. The criteria could also be optical OSNR. The maximum recovery time from the failure occurrence to the complete recovery of the optical link is far less than 50ms.

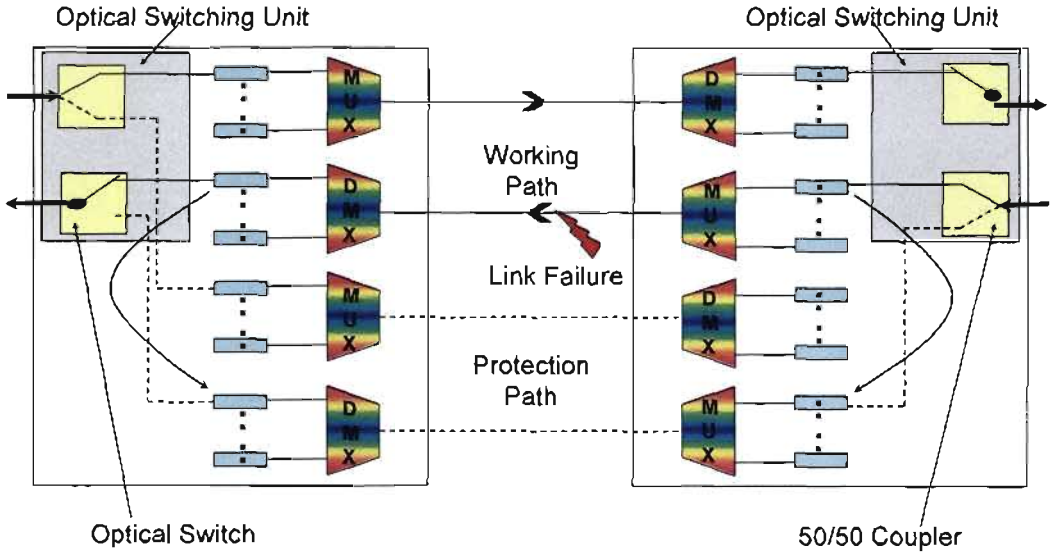


Figure 4-9 Optical 1:1 Channel Protection

The major advantage of optical channel protection is that optical channels are protected against fiber cuts as well as multiplexer/demultiplexer and transponder failures.

4.4.2.3 Optical Multiplex Section Protection

Optical Multiplex Section Protection is the most complex optical protection mechanism, where SONET/SDH restoration functions are implemented in DWDM ring systems. Reconfigurable DWDM add drop multiplexers provide dynamic wavelength channel allocation and protection switching to protect optical channels against network faults. As described by [22] Optical Unidirectional Path Switched Rings(O-UPSR) and Optical Bidirectional Line Switched Rings(O-BLSR) contribute greatly in this regard.

The O-UPSR architecture uses a two-fiber, counter rotating ring configuration. One fiber is used for protection wavelengths and the other is dedicated for working wavelengths. An O-UPSR uses 1 + 1 protection. A wavelength on the working and protection fiber is allocated and transmitted for each channel. The receiving side compares both optical signals and takes the one with the better optical signal to noise ratio. Figure 4-10 depicts a logical block diagram of an OADM using 1 + 1 protection in an O-UPSR.

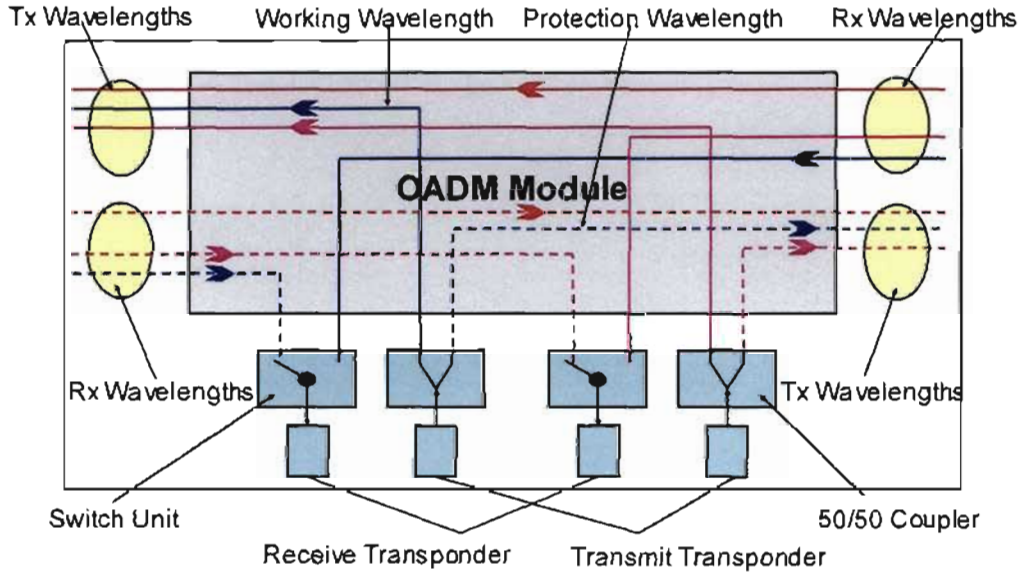


Figure 4-10 Reconfigurable OADM for 1+1 protection used in O-UPSR

The transmit transponder are connected to 50/50 couplers and each channel is split into a working and protection wavelength, which are then added to DWDM signal in the

ring by OADM module. The receiver transponders are connected to optical switch units, which select either the working or protection wavelength dropped by OADM module.

The O-BLSR architecture uses either a two or four fiber counter-rotating ring configuration. Within the two fibers O-BLSR, some wavelengths are used for allocating working channels, the remaining part is used as shared protection capacity. If a failure occurs, the reconfigurable ADM switches the failed wavelength onto a protection wavelength on the alternate path. If the number of working wavelengths equals the number of protection wavelengths, the O-BLSR uses 1:1 protection. A more efficient approach with regards to capacity is to use 1:n protection. In this way less than half the wavelengths are shared across the rest of the wavelengths for protection e.g. 1:3 protection in a 32 channel DWDM system, 24 wavelengths are protected by 8 wavelengths.

If 1:1 protection is being used, there are two possible wavelength allocation schemes. The first one uses same wavelengths for protection on both fibres in the ring. The second one uses for instance uses the lower half of the wavelengths for protection on the fiber in the clockwise direction and the other half on the fiber in the counter clockwise direction. The advantage of the latter one is that protection switching can occur without wavelength conversion in the OADM.

4.4.3 Restoration

Restoration can be seen as an overlaid mechanism, typical restoration can handle not only link failure but also node or multiple concurrent failures as opposed to protection. Restoration may be implemented in a centralised or distributed approach. In both instances, a network failure must be detected locally first, then the failure signal needs to be propagated to the control element controlling the restoration procedure. In general distributed restoration can restore failed services faster than centralised protection. Together with the use of pre-computed alternative paths, acceptable end to end restoration times can be achieved. Mesh-based distributed restoration is generally the choice for implementation in optical networks. Restoration is generally accomplished at either layer 2 or layer 3.

4.4.3.1 Restoration Time ITU-T M.495

A key criterion that needs to be considered for achieving a survivable network is the restoration speed. The ITU-T recommendation M.495 "Maintenance: International Transmission Systems"[ITU-5] specifies how the restoration time is calculated.

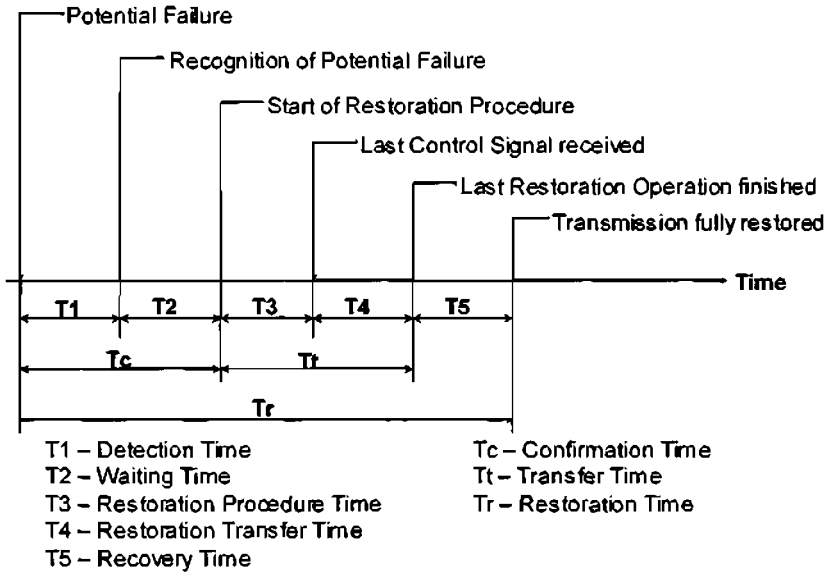


Figure 4-11 Restoration time components according to ITU-T M.495

In case of a failure, it takes some time until the network node next to the failure detects the failure and triggers, for example, a Loss of Signal(LOS) or Signal Degrade(SD) event. This time interval is called the Detection Time(T1).

After some time the failure is confirmed, and the restoration procedure is initiated. The time interval between this point of time and the failure recognition is called the Waiting Time(T2).

The time interval between the failure and occurrence and the fault confirmation is called the Confirmation Time(Tc).

During the Restoration Procedure Time(T3), control signals are transmitted and received signals are processed.

The amount of time required for processing the last received control signal called the Restoration Transfer Time(T4).

The time interval between the fault confirmation and the point of time until the last restoration operation is finished is called the Transfer Time(T4).

In the last step, a verification of the protection switching operation or some resynchronisation might be completed. This time is called the Recovery Time (Tr).

As an example, the detection time for SONET/SDH is specified with $10ms$ and restoration time with $60ms$. As a consequence, equipment used to deploy SONET/SDH networks must detect failure within $10ms$ and restore traffic within $50ms$. As highlighted earlier in this chapter all optical networks are striving to improve on these times.

4.4.3.2 Comparison of Survivability Mechanisms

There are various design criteria to be taken account of when considering the various survivability architectures. The following tables are used to provide a basic comparison of the survivability mechanisms in IP, ATM and SONET networks as well as Optical Transport Networks (OTN).

	MPLS Restoration	Standard IP Routing Restoration	ATM PNNI Restoration	SONET/SDH Shared Protection	SONET/SDH Dedicated Protection
Restoration Time	$50ms..1s$	$1..10s$	$1..10s$	$<100ms$	$<100ms$
Restoration Capacity	0..100%	~ 0%	~ 0%	<100%	100%
Restoration Capacity Usable by Low-Priority Traffic	Yes	N/A	N/A	Yes	No(UPSR) Yes(APS)
Linear Topologies	Yes	Yes	Yes	Yes	Yes
Ring Topologies	Yes	Yes	Yes	Yes	Yes
Mesh Topologies	Yes	Yes	Yes	No	No

Table 4-2 Survivability Mechanisms Comparison for IP,ATM and SONET Networks

Typical figures for design criteria are presented in Table 4-1, key points to note are the poor restoration capacity usage as well as the relatively high restoration times. Although these figures are not exact it gives a fair indication of the short comings of the survivability mechanisms for these types of networks.

	OCH Protection	**OMS Shared Protection**	**OMS Dedicated Protection**	**Line Protection**
Restoration Time	$< 50ms$	$< 200ms$	$< 200ms$	$< 50ms$
Restoration Capacity	100%	<100%	100%	100%
Restoration Capacity Usable by Low-Priority Traffic	No	Yes	Yes(O-APS) No(O-UPSR)	No
Linear Topologies	Yes	Yes	Yes	Yes
Ring Topologies	Yes	Yes	Yes	N/A
Mesh Topologies	Yes	No	No	N/A

Table 4-3 Survivability Mechanisms Comparison for Optical Transport Networks(OTN)

On average the restoration times are lower and restoration capacity higher for Optical Transport Networks compared to IP, ATM and SONET. These parameters are good indicators of the networks ability to recover from failures and hence are directly linked to determining the level of survivability that can be offered by a specific type of network. Clearly if one where to choose a network that would offer high survivability in terms of how fast a network restores a failure OTN's would be the network of choice. With most Service Level Agreements(SLA) being based on the amount of guaranteed service that can be offered by the network, OTN's offer good survivability mechanisms to ensure that these SLA's are met.

Chapter 5

Testing and Simulation

In this chapter the aim is to conduct simulations using the WDM Guru software to try and ascertain which protection scheme exhibits the best performance under varying conditions such as link and node failure as well as varying traffic loads. As explained in preceding chapters protection is one of the mechanisms employed to achieve survivable networks. Availability analysis is also conducted; this analysis is used to calculate the service availability in the network. The values obtained from service availability can be used to verify the degree to which the service level agreements are being met. The results obtained in this chapter will be used to evaluate the robustness of the various protection schemes to failure, this together with the data obtained from the various experiments will be used to make recommendations and highlight pitfalls of the various protection schemes.

5.1 Description of Network

A 14 node 23 link network is being used to simulate the various protection schemes, in particular 1+1dedicated path protection, shared path protection, path restoration and link restoration are being simulated.

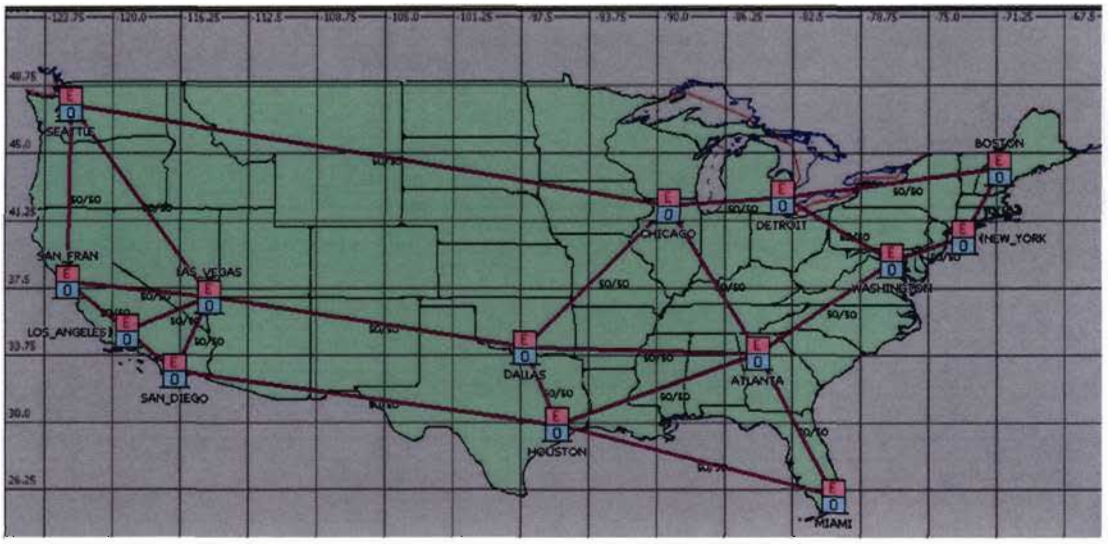


Figure 5-1 Network used in simulation

The nodes in the network are denoted by city names and the links are illustrated by purple lines. Each link represents a fiber cable with 50 fiber pairs within it. Each fiber is capable of carrying 40 wavelengths. The och-40 traffic matrix is used to simulate traffic in the network.

5.2 Simulation Approach

The fundamental aim of the simulations in this chapter is to analyse the performance of the various protection schemes by varying certain parameters such as number of nodes or links failed, varying traffic loads and analysing service availability.

5.2.1 Node/Link Failure

This type of failure provides a means of testing the performance of the protections schemes by failing nodes or links and observing the ability of the various schemes to recover from these failures.

The performance is judged by analysing the following:

1. total number of wavelengths affected by node/link failure
2. total number of wavelengths lost by node/link failure
3. total number of wavelengths recovered by node/link failure

The WDM software allows us to fail links at random and then evaluate the effect these failures have on the wavelengths being transmitted in the network.

5.2.1.1 Rationale for choice of Link Failures

Three options could be used for choosing which links to fail:

1. Choose the links with the longest distance, by using this as a choice we are testing for worst case scenario since the longer the cable the greater the delay as illustrated by the link browser table A-1 in Appendix A and hence failing the cable would result in the traffic taking a longer time to be rerouted.

2. Choose the links with the shortest distance, by using this choice we would not really be testing the protection scheme since short links exhibit lower delays.
3. Try to choose equal number of long and short links in a well distributed random manner, by choosing in this fashion we are mimicking the possible failures in a real optical network. Also in doing so the protection schemes will be adequately tested.

For the simulations done regarding link/node failure, option 3 was chosen.

5.2.2 Service Availability

For this simulation WDM Guru considers all possible network failures and, for each failure, evaluates which part of the traffic can be recovered. The system correlates the data with the probability of each failure. The probability is calculated according to the specified failure rates for the equipment. The system then reports the availability for each connection. Also, it reports the expected loss of traffic of the entire traffic matrix, given the specified protection method. This feature is fundamental to ensuring that the service level agreement is upheld, it also gives a fair indication as to which protection scheme would best be suited to offer for example a 99.99% network availability.

5.2.3 Traffic Variations

Like in any real network, traffic is always changing, hence in order to give a proper evaluation of the performance of the protection schemes they had to be evaluated under varying traffic loads. The effect of varying traffic levels on the network can be predicted, and the network's performance for different protection strategies can be assessed.

This operation does not add resources to the network; it determines how the existing network will handle projected traffic variations. When it simulates the effects of traffic variations, WDM Guru takes node, link, and tributary capacity into account. In a typical network, traffic is usually dynamic hence these variations can be used to test the various protection schemes to ascertain their performance to varying traffic loads.

5.3 Simulation Results: Failure Analysis

5.3.1 CASE 1 – Link Failure

The unprotected scenario was the first scenario considered to observe the values of recovered and lost wavelengths under the worst case scenario namely the one without protection. There after the order of analysis was dedicated path protection, shared path protection, path restoration and link restoration. Each of these protection schemes were analyzed under varying percentages of failure.

In order for results to be coherent the same links that were failed at a specific percentage for a particular scheme was failed for the rest the schemes, for example, if we failed the links Dallas-Texas and Los Angeles-Houston at 10% failure for the unprotected scheme the same links were failed for the remaining protection schemes see Appendix B1.

5.3.1.1 10% Link Failure

The base model used for all simulations in Figure 5-1 consists of 23 links in total; hence a 10% link failure will result in approximately 2 links failing in the network. The following figure illustrates the network used in the simulation of 10% link failure. The links from Los Angeles-San Diego and Seattle-Chicago were failed, note failure was chosen randomly and one short link as well as one long link was chosen.

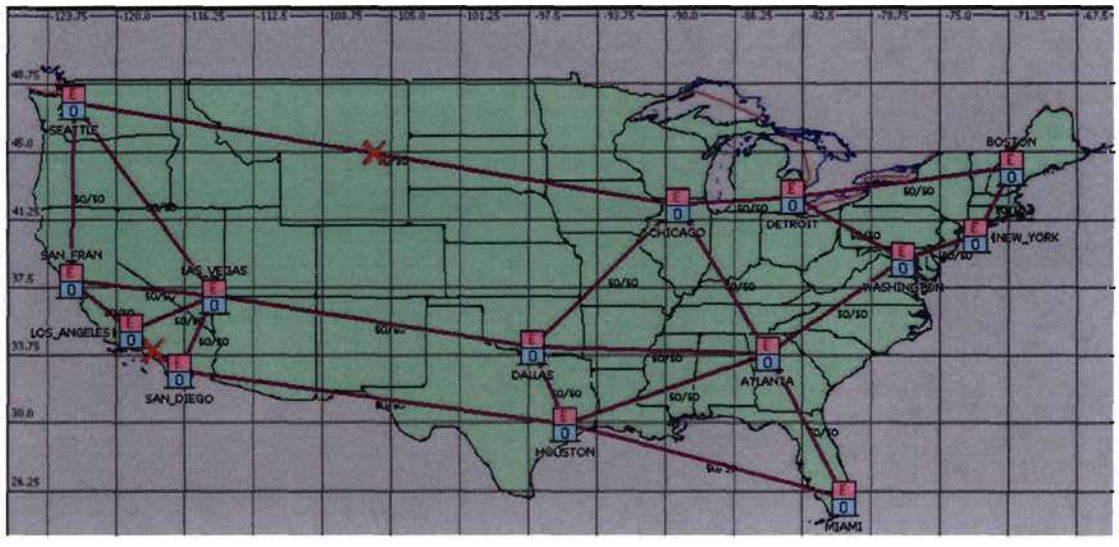


Figure 5-2 Model for 10% Failure of Links

The results in Table 5-1 were obtained for the different protection schemes at 10% link failure.

Protection Scheme	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
Unprotected	15	15	0
Dedicated Path	28	0	28
Shared Path	28	6	22
Path Restoration	18	0	18
Link Restoration	32	18	14

Table 5-1 Results for 10% Link Failure

Table 5-1 is used for illustration purposes, so that insight into the manner in which the results tabulated below were obtained. The results clearly show that unprotected case at 10% performs the worst in terms of wavelength recovery. The clear winner in terms of wavelength recovery is dedicated protection. This was expected since in this scheme protection is achieved by assigning a back up path to every working path.

The results for all simulation with respect to link failures ranging from 10%-80% for the various protection schemes are tabulated in the sections below. For further information regarding the scenario models and links failed for each scenario refer to Appendix B1 and for detailed reports with respect to the rerouted traffic see attached CD Rom Appendix B1-1.

5.3.1.2 Scenario 1 - Unprotected

In this scenario no protection scheme is applied to the model network in Figure 5-1, links are failed at varying percentages and results are tabulated below. This scenario is the worst possible, since there is protection scheme in place to assist in the recovery of the network in the event of a failure.

Percentage Failure	Number of nodes failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	2	15	15	0
20	5	31	31	0
30	7	59	59	0
40	9	78	78	0
50	12	92	92	0
60	14	123	123	0
70	16	128	128	0
80	18	139	139	0

Table 5-2 Results of Unprotected scheme under varying percentage failures

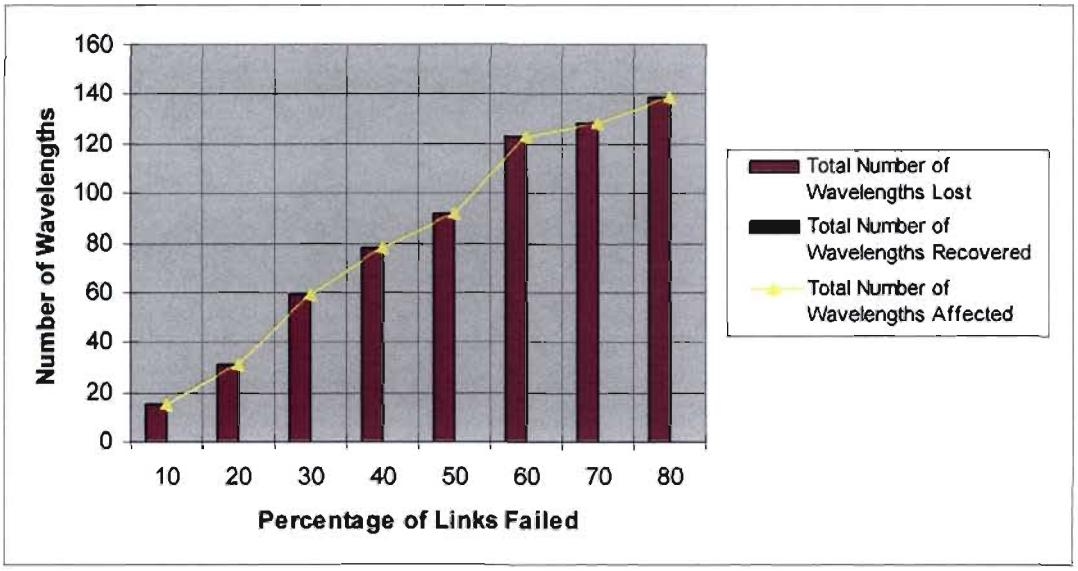


Figure 5-3 Analysis of link failure for unprotected scenario

From Figure 5-3, we can see that the unprotected protection scheme cannot recover from any amount of link failure. Data travelling on these links would be completely lost since no wavelengths were recovered.

5.3.1.3 Scenario 2 - Dedicated Path Protection

In this scenario Dedicated Path Protection scheme is applied to the model network in Figure 5-1, links are failed at varying percentages and results are tabulated below

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	2	28	0	28
20	5	42	8	34
30	7	63	34	29
40	9	81	52	29
50	12	93	71	22
60	14	124	116	8
70	16	130	130	0
80	18	141	141	0

Table 5-3 Results of Dedicated protection scheme under varying percentage failures

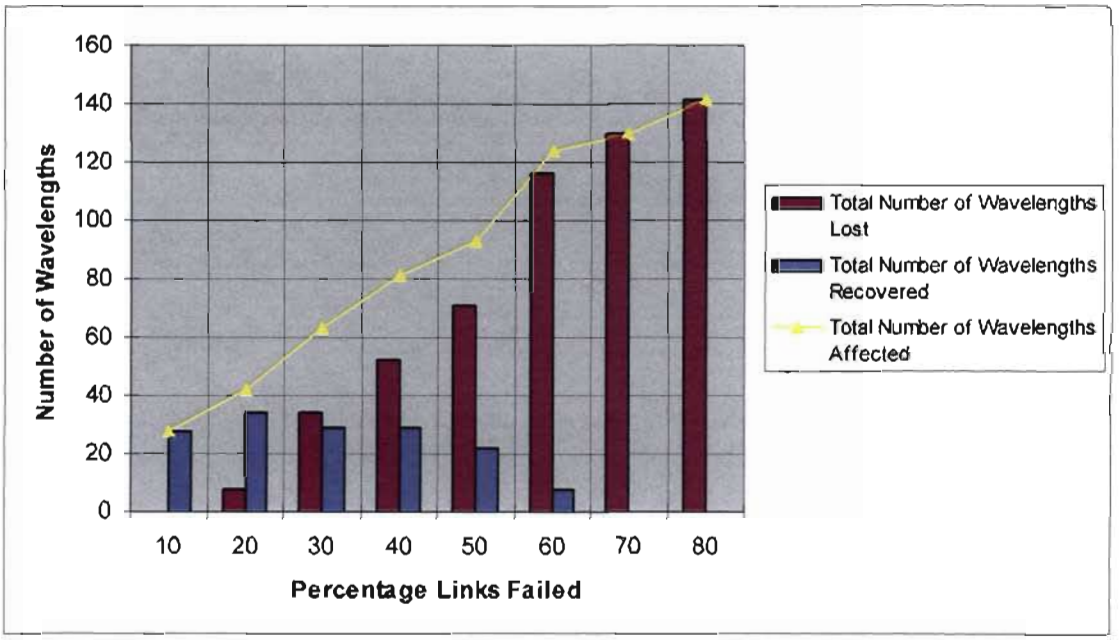


Figure 5-4 Analysis of link failure for Dedicated Path Protection

The Dedicated Path Protection scheme offers good recovery to failures up until 60% in fact it is able to recover all wavelengths at 10% failure. A fairly high amount of wavelengths are affected at any given percentage failure in this protection scheme. This is expected due to the high capacity needed for this type of protection.

5.3.1.4 Scenario 3 - Shared Path Protection

In this scenario Shared Path Protection is applied to the model network in Figure 5-1, links are failed at varying percentages and results are tabulated below

Percentage Failure	Number of Nodes failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	2	28	6	22
20	5	42	13	29
30	7	63	37	26
40	9	81	55	26
50	12	93	72	21
60	14	124	116	8
70	16	130	130	0
80	18	141	141	0

Table 5-4 Results of Shared Path Protection scheme under varying percentage failures

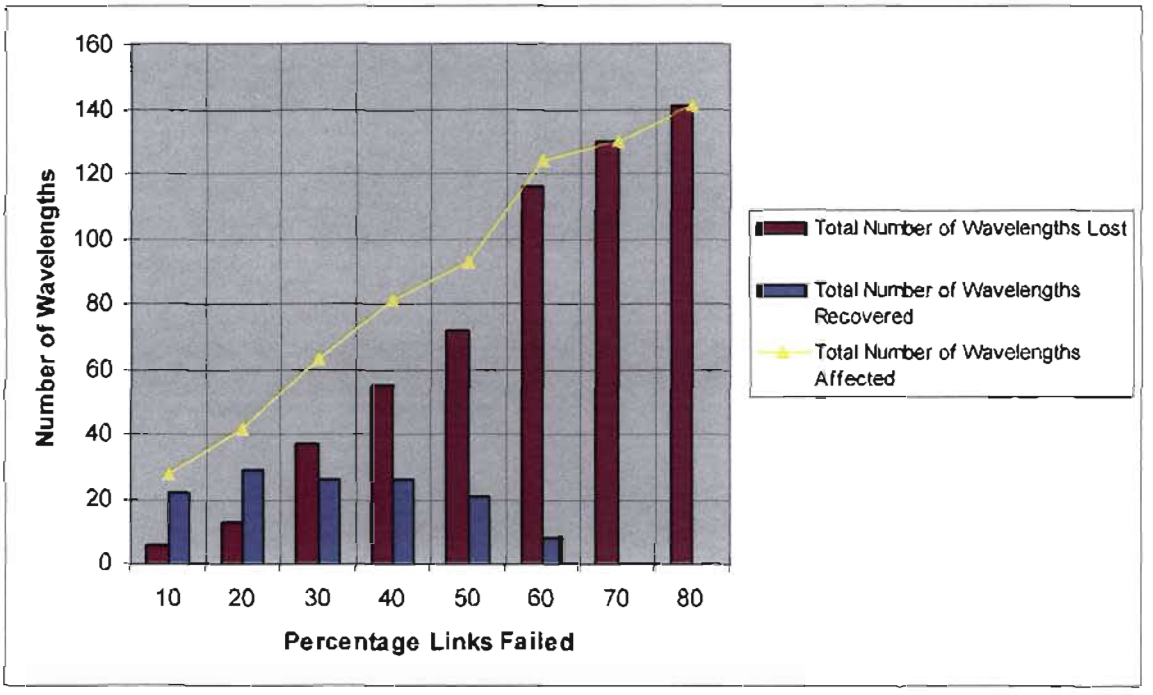


Figure 5-5 Analysis of link failure for Shared Path Protection scenario

In this scenario the Shared Path Protection scheme offers some form of protection across the various percentage failures. A fairly high amount of wavelengths are affected at any given percentage failure in this protection scheme as well. This is expected due to the use of a predefined working path and protection path, the key difference here is that traffic is only routed on the working path and is switched to the protection path when failure occurs.

5.3.1.5 Scenario 4 - Path Restoration

In this scenario Path Restoration is applied to the model network in Figure 5-1, links are failed at varying percentages and results are tabulated below

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	2	18	0	18
20	5	34	12	22
30	7	62	32	30
40	9	76	41	35
50	12	92	74	18
60	14	123	114	9
70	16	128	128	0
80	18	139	139	0

Table 5-5 Results of Path Restoration scheme under varying percentage failures

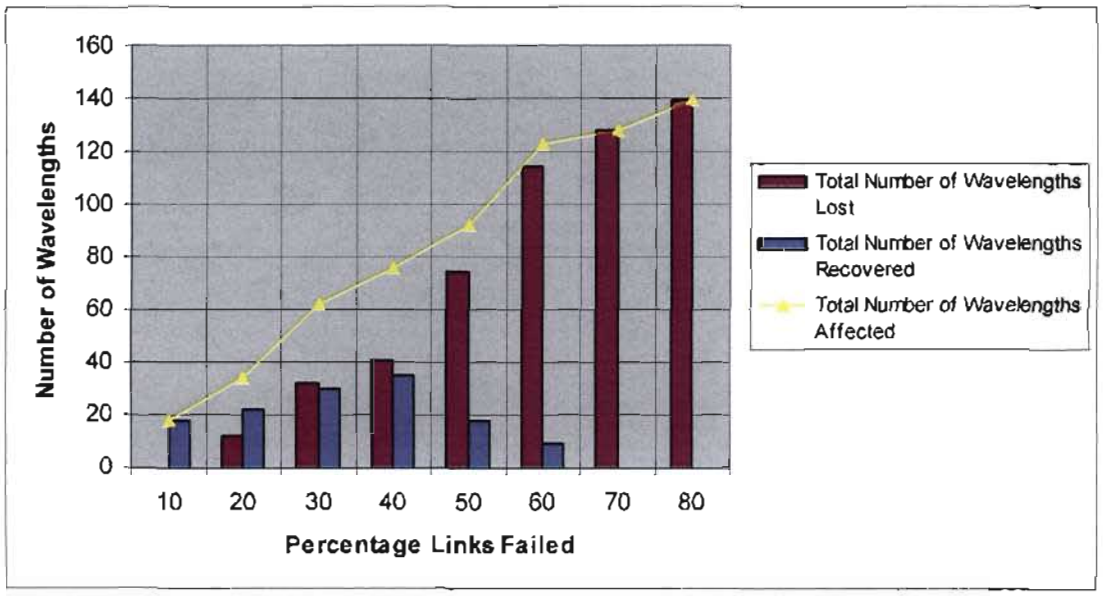


Figure 5-6 Analysis of link failure for Path Restoration scenario

The Path Restoration offers good recovery to failures up until 60% in fact it is also able to recover all wavelengths at 10% failure. The amount of wavelengths that are affected at any given percentage failure in this protection scheme is slightly lower. This can be attributed

to the fact that when a link fails this protection scheme reroutes each connection individually around the failing entity between the end-points of the connection.

5.3.1.6 Scenario 5 - Link Restoration

In this scenario Link Restoration is applied to the model network in Figure 5-1, links are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	2	18	0	18
20	5	34	15	19
30	7	62	19	43
40	9	78	33	45
50	12	92	67	25
60	14	123	103	20
70	16	128	128	0
80	18	139	139	0

Table 5-6 Results of Link Restoration scheme under varying percentage failures

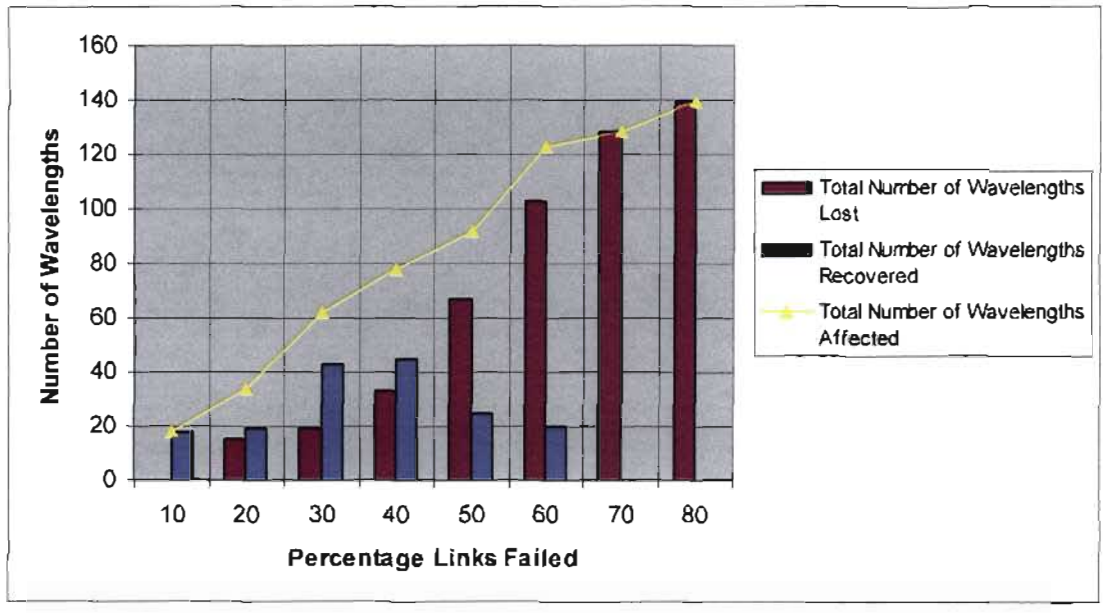


Figure 5-7 Analysis of link failure for Link restoration

From Figure 5-7 it can be seen that Link Restoration offers good recovery to failures up until 60%. At 10% it also recovers all wavelengths affected by the link failure. Restoration paths and rerouting is done only when a failure occurs as a result restoration capacity is shared on all network links. The number of wavelengths recovered from failures around 30% to 60% is high, this could be attributed to the fact that if rerouting in Link Restoration is successful, all connections routed over the failed link are restored at the same time.

5.3.1.7 Analysis of total number of wavelengths affected for all protection schemes

Figure 5-8 is a comparative analysis for each of the protected and unprotected scenarios.

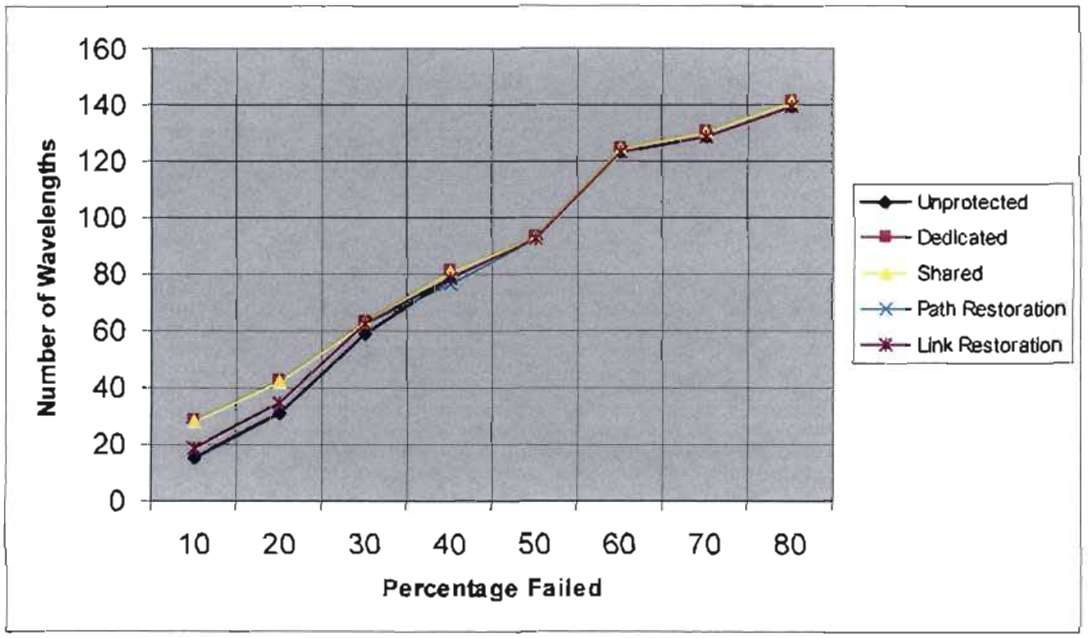


Figure 5-8 Comparative Analysis of Affected Wavelengths under varying Protection Schemes

By visual analysis, we see that during varying percentages of link failure the most amount of wavelengths are affected by shared and dedicated protection; from explanations given above, these results follow since these protection schemes utilize the most capacity due to them having pre-established backup paths. Link restoration seem to have the least amount of affected wavelengths as compared to the other schemes, this is largely due to the fact that network resource are shared when implementing this scheme.

5.3.1.8 Analysis of total number of wavelengths recovered for all protection schemes

From theory dedicated protection offers the best protection for low percentage of failures. Figure 5-9 gives a comparative analysis as to which scheme provides the best wavelength recovery at varying percentages of failure.

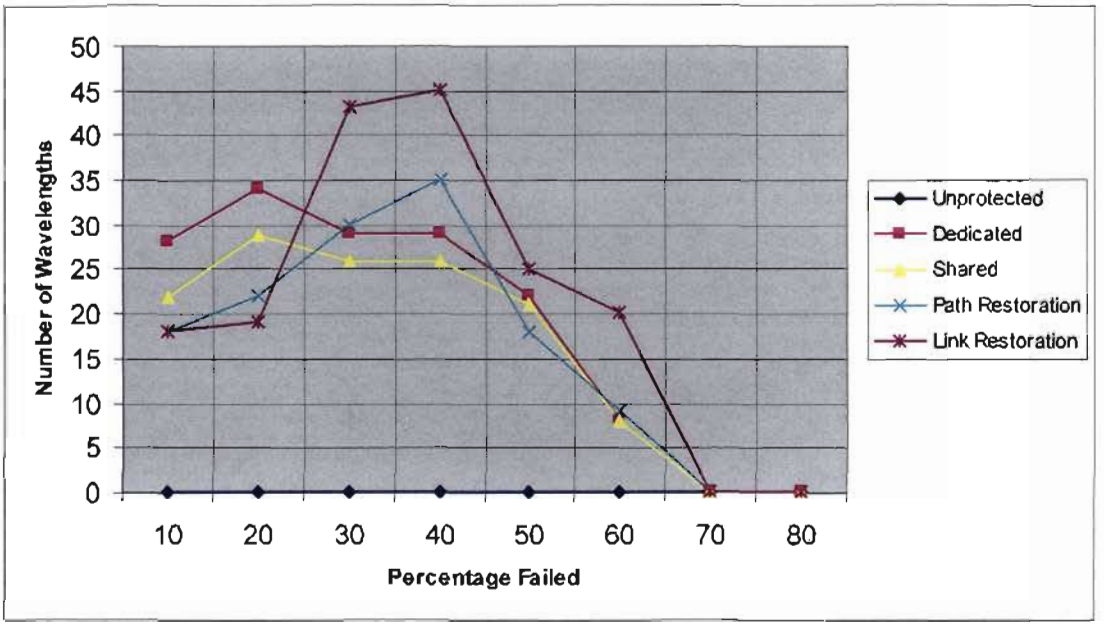


Figure 5-9 Comparative Analysis of Recovered Wavelengths under varying Protection Schemes

These results provide a relatively good indication of the performance of the different protection schemes with regards to wavelength recovery under varying percentages of failure. Dedicated protection does prove to be the most effective protection method at low percentage of failures; however, Link Restoration is most effective at high degrees of a failure, as illustrated in Figure 5-9.

5.3.1.9 Discussion of Results for Link Failure

The above simulations have led to a number of important observations and conclusion.

a. Dedicated Protection and Shared Protection offer good protection to link failures from 0%-25% link failures. Thereafter, as percentage of failures increase its

performance deteriorates, this can be attributed to the fact that these schemes utilize pre-determined back up paths. Hence when the number of links that are being failed increases these predetermined backup paths are adversely affected as well and hence, failed wavelengths cannot be rerouted.

b. At failures above 25%, Link Restoration performs the best in terms of number of wavelengths recovered. During failures it also exhibits the lowest amount of wavelengths affected. This scheme obviously displays much more adaptability to high failures and as a result will be effective in making the network more survivable at high link failures.

c. From the tabulated results, dedicated, path restoration and link restoration are able to recover totally from 10% link failure since all affected wavelengths were recovered.

5.3.2 CASE 2 - Node Failure

In this case the simulation procedure and order of analysis was identical to that used for link failures, the key difference was that instead of failing the links we now fail the nodes and analyze the protection schemes.

5.3.2.1 10% Node Failure

The nodes generally handle most of the routing and wavelength assignment functions, they also serve as an interface between connections, hence a failure at any one node affects all connections coming into and leaving it.

The base model used for all simulations in Figure 5-1 consists of 14 nodes in total; hence a 10% node failure will result in approximately 1 node failing in the network. The following figure illustrates the network used in the simulation of 10% node failure. The Seattle node was failed.

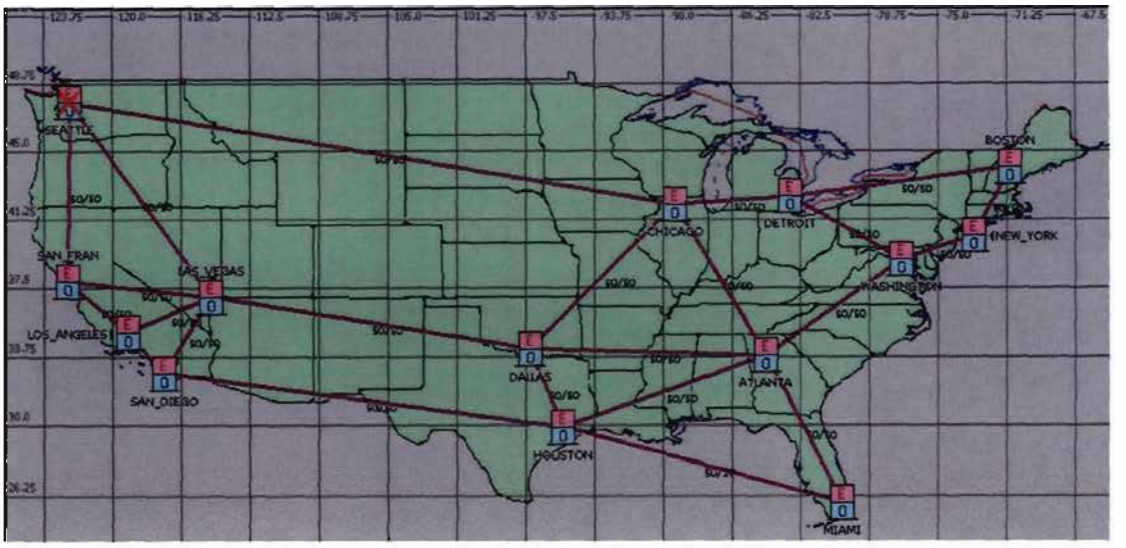


Figure 5-10 Model for 10% Failure of Nodes

The following results were obtained for the different schemes at 10% node failure.

Protection Scheme	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
Unprotected	29	29	0
Dedicated Path	36	21	15
Shared Path	36	21	15
Path Restoration	29	21	8
Link Restoration	29	29	0

Table 5-7 Results for 10% Node Failure

Table 5-7 is used for illustration purposes, so that insight into the manner in which the results tabulated below were obtained.

The results for all simulation with respect to node failures ranging from 10%-80% for the various protection schemes are tabulated in the sections below. For further information regarding the scenario models and nodes failed for each scenario refer to Appendix C1 and for detailed reports with respect to the rerouted traffic see attached CD Rom Appendix C1-1.

5.3.2.2 Scenario 1 - Unprotected Scheme

In this scenario to test node failure, no protection scheme is applied to the model network in Figure 5-1, nodes are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	1	29	29	0
20	3	109	109	0
30	4	114	114	0
40	6	134	134	0
50	7	146	146	0
60	8	149	149	0
70	10	151	151	0
80	11	154	154	0

Table 5-8 Results of Unprotected scheme under varying percentage failures

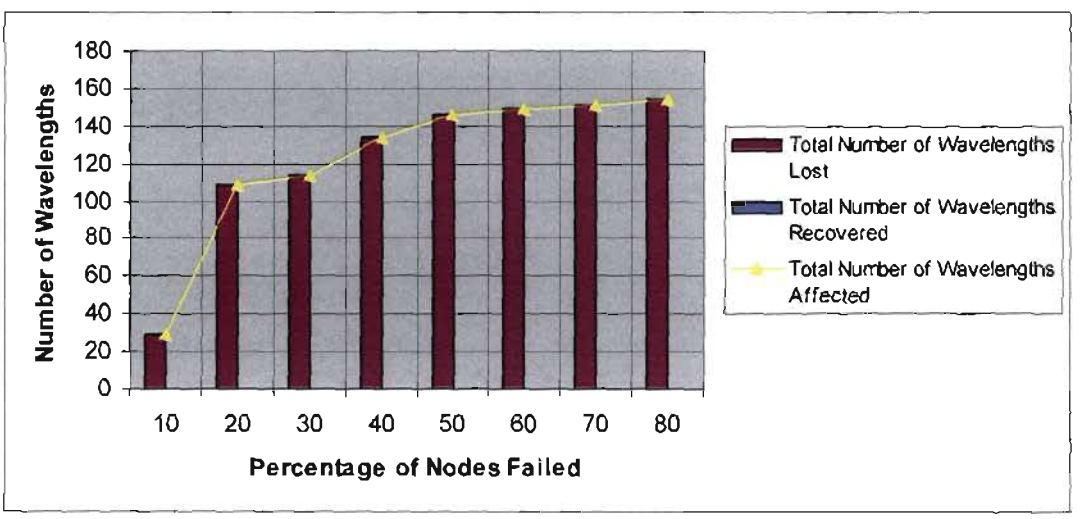


Figure 5-11 Analysis of node failure for Unprotected Scenario

From Figure 5-11, we can see that the unprotected protection scheme cannot recover from any amount of node failures. Data travelling on links associated with the failed node would be completely lost since no wavelengths were recovered. The total number of wavelengths affected is equal to the number of wavelengths lost.

5.3.2.3 Scenario 2 - Dedicated Path Protection

In this scenario to test node failure, Dedicated Path Protection is applied to the model network in Figure 5-1, nodes are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	1	36	21	15
20	3	110	84	26
30	4	118	99	19
40	6	134	122	12
50	7	146	141	5
60	8	149	146	3
70	10	151	151	0
80	11	154	154	0

Table 5-9 Results of Dedicated Path protection scheme under varying percentage failures

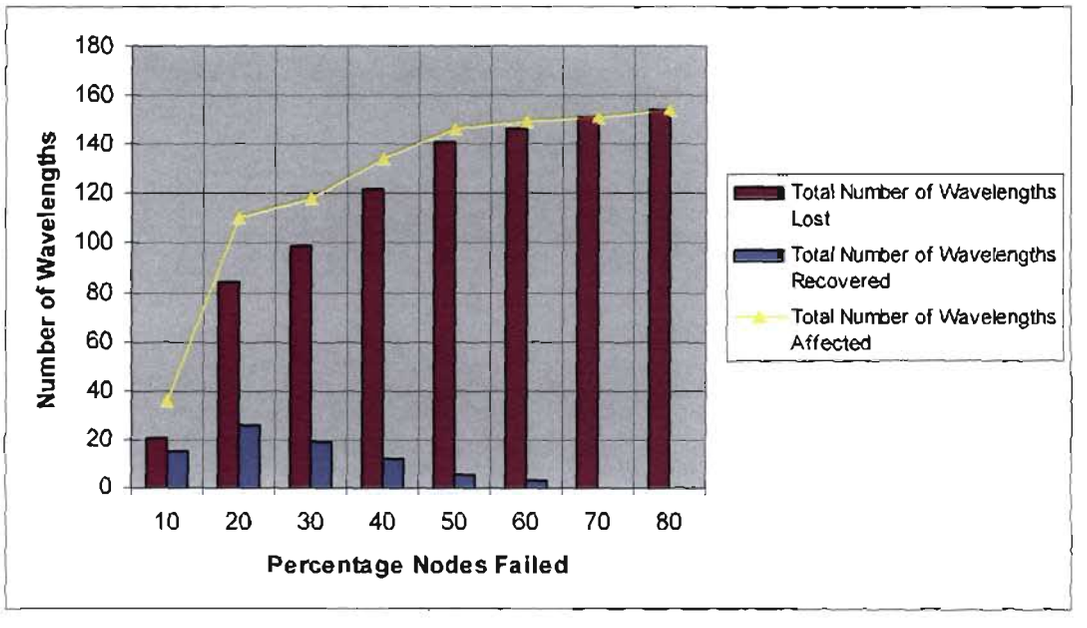


Figure 5-12 Analysis of node failure for Dedicated Protection scenario

The Dedicated Path Protection scheme offers good recovery up until 60% node failures. A fairly high amount of wavelengths are affected at any given percentage failure in this

protection scheme. This is expected due to the nature of this scheme to use pre-defined restoration paths to recover from failures.

5.3.2.4 Scenario 3 - Shared Path Protection

In this scenario to test node failure, Shared Path Protection is applied to the model network in Figure 5-1, nodes are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	1	36	21	15
20	3	110	85	25
30	4	118	100	18
40	6	134	122	12
50	7	146	141	5
60	8	149	146	3
70	10	151	151	0
80	11	154	154	0

Table 5-10 Results of Shared Path Protection scheme under varying percentage failures

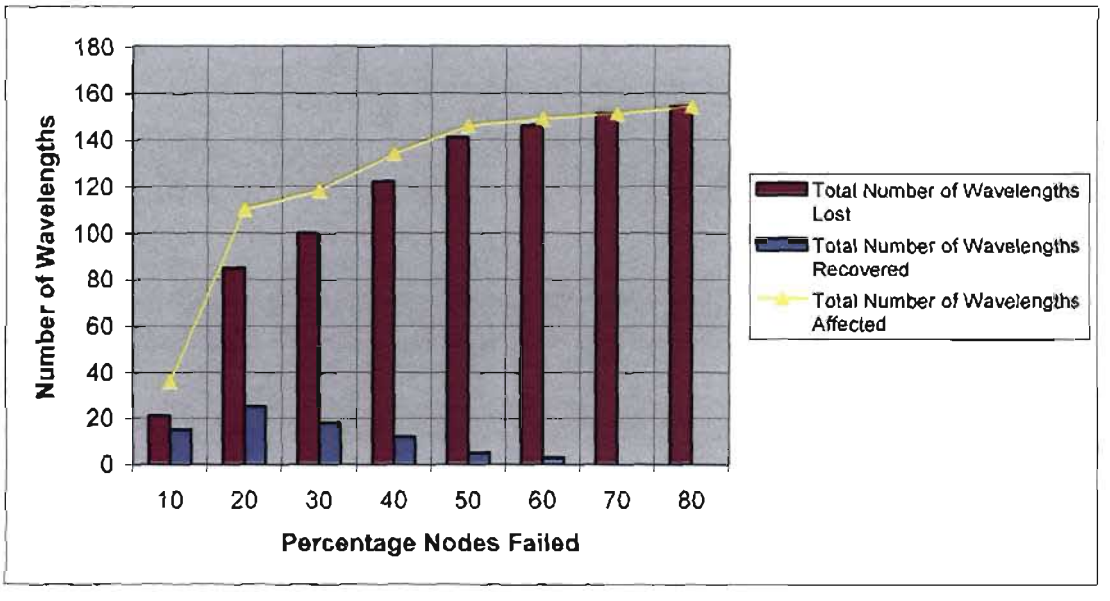


Figure 5-13 Analysis of node failure for Shared Path Protection scenario

In this scenario the Shared Path Protection scheme offers some form of protection across the various percentage node failures. A fairly high amount of wavelengths are affected at

any given percentage failure in this protection scheme as well. This is expected due to the use of a predefined working path and protection paths, the key difference here is that traffic is only routed on the working path and is switched to the protection path when failure occurs, this scheme will be able to recover affected wavelengths up until 60% failures.

5.3.2.5 Scenario 4 - Path Restoration Scheme

In this scenario to test node failure, Path Restoration Protection is applied to the model network in Figure 5-1, nodes are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	1	29	21	8
20	3	109	77	32
30	4	114	85	29
40	6	134	109	25
50	7	146	136	10
60	8	150	146	4
70	10	151	151	0
80	11	154	154	0

Table 5-11 Results of Path Restoration scheme under varying percentage failures

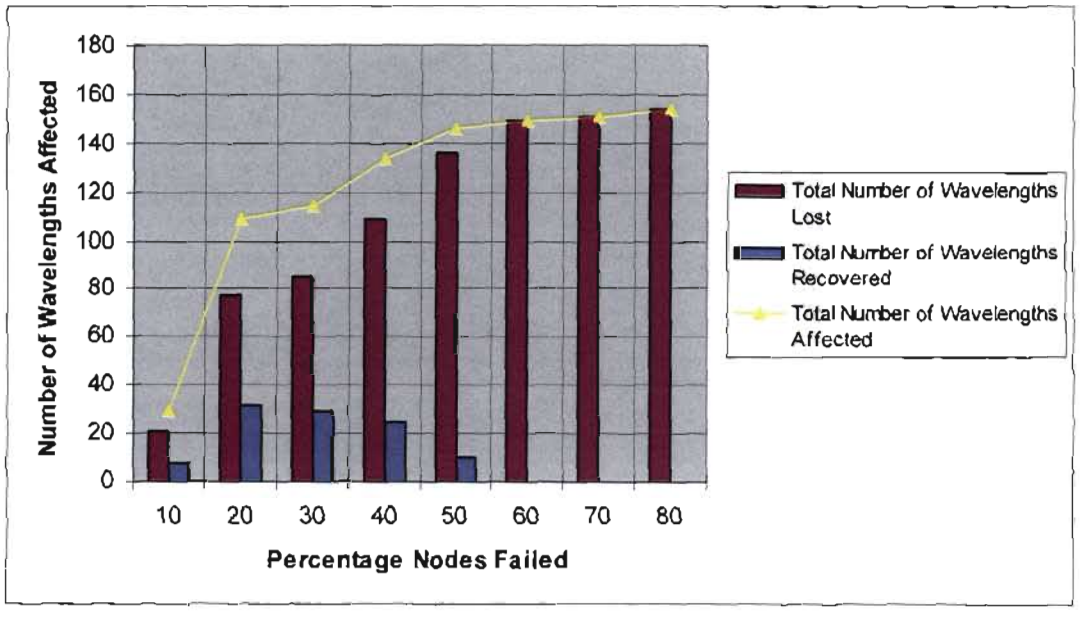


Figure 5-14 Analysis of node failure for Path Restoration scenario

The Path Restoration offers good recovery only up until 50% failures. The number of wavelengths that are affected at any given percentage failure in this protection scheme is equal to the other schemes. Failure at any of the nodes results in a fewer number of alternate paths being available for restoration, when a node fails this protection scheme reroutes each connection individually around the failing entity between the end-points of the connections.

5.3.2.6 Scenario 5 - Link Restoration Scheme

In this scenario to test node failure, Link Path Protection is applied to the model network in Figure 5-1, nodes are failed at varying percentages and results are tabulated below.

Percentage Failure	Number of Nodes Failed	Total Number of Wavelengths Affected	Total Number of Wavelengths Lost	Total Number of Wavelengths Recovered
10	1	18	29	0
20	3	109	109	0
30	4	114	114	0
40	6	134	134	0
50	7	146	146	0
60	8	149	149	0
70	10	151	151	0
80	11	154	154	0

Table 5-12 Results of Link Restoration scheme under varying percentage failures

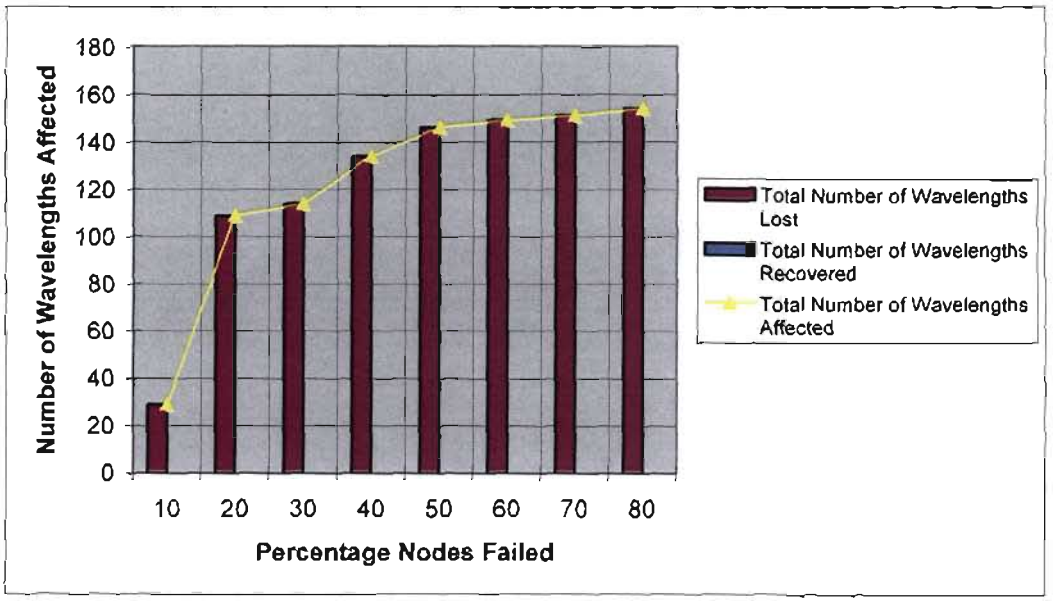


Figure 5-15 Analysis of node failure for Link Restoration scenario

dedicated and shared path performance deteriorates, this can be attributed to the fact that these schemes utilize pre determined back up paths.

2. Path restoration seems to be able to handle the higher percentage of failures more effectively in terms of wavelength recovery. Its does however reach its saturation point faster than dedicated and shared path protection.
3. Across all percentage failures the number of wavelengths affected in the path restoration scheme is the least. This scheme obviously displays much more adaptability to high node failures and as a result will be effective in making the network more survivable at node failures between 10%-60%.

5.4 Simulation Results: Link Availability Analysis

In the results presented in this section are intended to indicate which protection scheme provides the best service availability. Service availability is a key consideration in designing survivable networks since, most clients are interested in the ability of the network to meet a specific degree of availability, this degree of availability is of referred to as the Service Level Agreement. For the simulations carried out to evaluate service availability certain parameters had to be pre defined these are:

1. Cable Length Per Cut Per Year
2. Mean Time To Repair

Cable Length per Cut per Year refers to the average estimated cable length (km), within which you expect a single cable cut to occur over a year. The Mean Time To Repair (MTTR) (hours) indicates the mean time it takes to repair the cable cut, for example if we specify a cable length per a cut to be 200km and a MTTR of 12 hours this would mean that a cable cut would occur at some point every 200km over the link over the next year, and each cut will take 12 hours to repair. Thus a link that is 800 km long will experience four cuts over the year and each cut will take 12 hours to repair hence the total downtime of the network would be 96 hours.

The following are the values were assumed:

Cable Length per Cut per Year = 300 kilometres
Mean Time to Repair = 12 hours

For the purposes of this simulation since we are focused on the effects of link failures only, the availability of equipment is set to 1, hence no equipment failures are taken into account accept cable cuts. Table 5-13 contains results obtained from simulating network availability for the various protection schemes using the above assumed values.

Protection Scheme	Average Availability	Expected Loss In Traffic (Gb/year)
Unprotected	0.988147018	143,220,548.70
Dedicated	0.999775872	2,708,163.20
Shared Path Protection	0.998853254	13,856,229.50
Path Restoration	0.999345238	7,911,541.80
Link Restoration	0.999706856	3,542,089.10

Table 5-13 Average availability and Expected Loss in Traffic

The Figure 5-18 is a plot of the average availability offered by the various protection schemes, after taking into account the cable length per cut per year and mean time to repair these failures

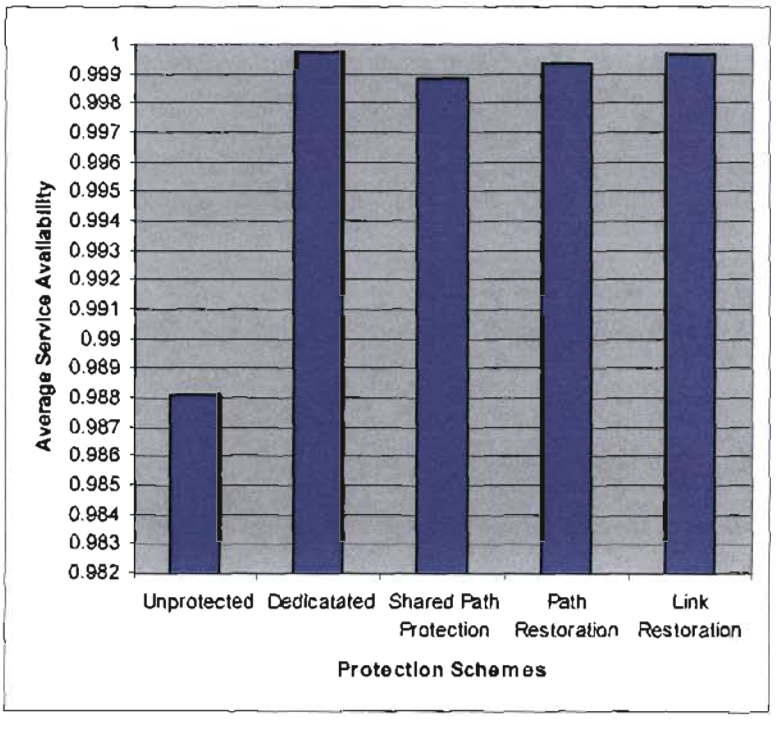


Figure 5-18 Average Availability offered by various Protection schemes

The order of increasing average service availability is as follows, the highest average service availability is offered by dedicated protection, thereafter link restoration, path restoration and shared path protection and lowest average service availability is offered by unprotected scheme, this is mainly attributed to the fact that there is no protection scheme in place for when cable cuts occur.

The graph presented in Figure 5-19 is a representation of the data in Table 5-13 for the expected loss in traffic annually after taking into account the cable length per cut per year and mean time to repair these failures for each of the protection schemes. The unprotected scheme stands to lose the most amount of traffic; this would be expected since no protection is applied here. The order of increasing loss in traffic of the various schemes is as follows, dedicated, link restoration, path restoration and shared path protection. Dedicated protection offers the least amount of traffic loss mainly because of the pre-defined protection path that it uses in event of a failure; however what is interesting to note that even though link restoration does not apply pre-determined backup paths for restoration it still performs better than shared path protection which does employ pre-defined protection paths.

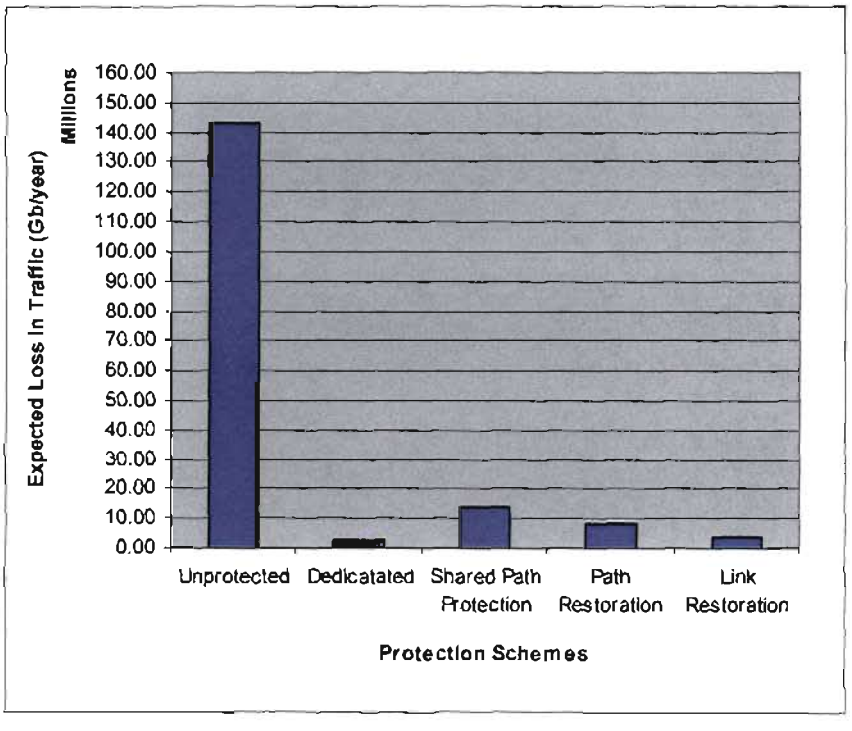


Figure 5-19 Expected Loss in Traffic Annually for Protection schemes

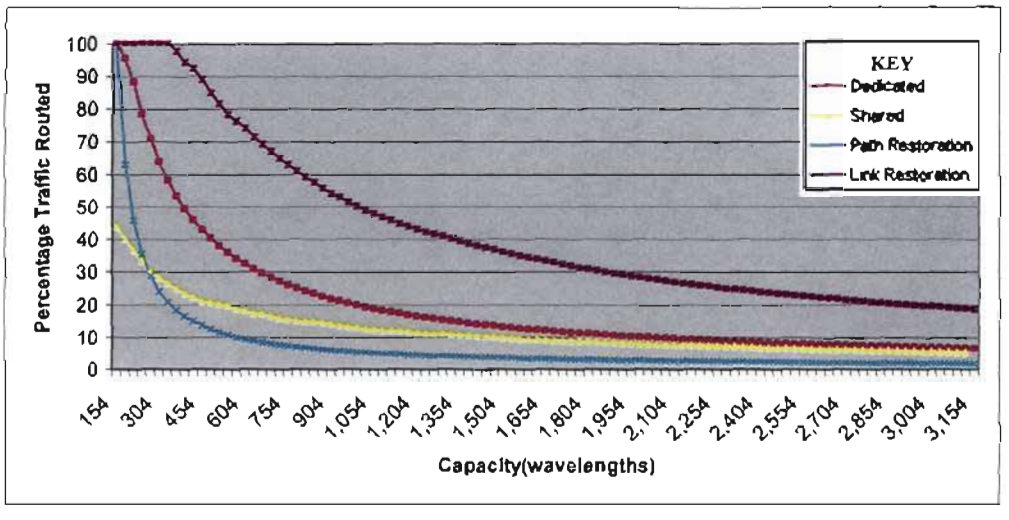
5.4.1 Discussion of Results for Link Availability Analysis

The above simulations have led to the following important observations;

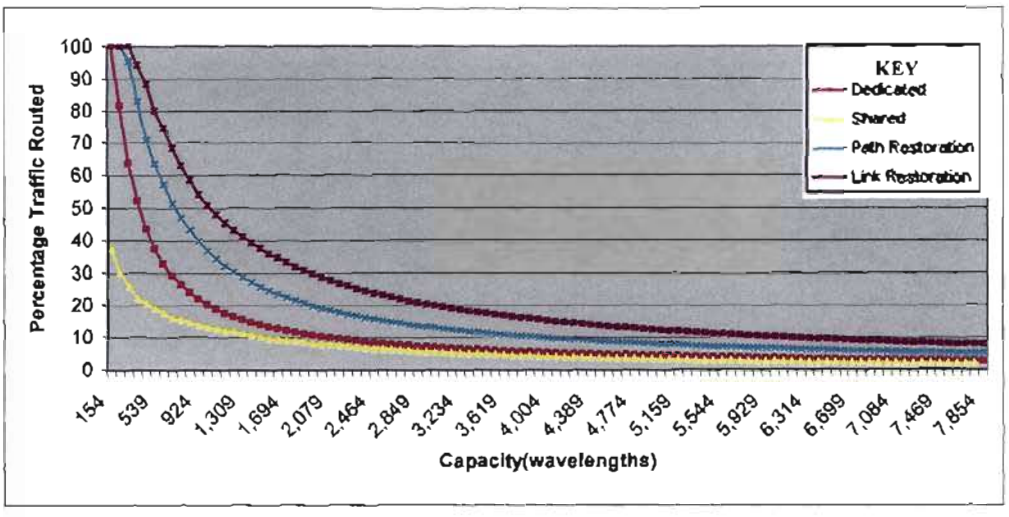
1. Dedicated protection offers the best average service availability as well as the lowest expected loss in traffic.
2. Link Restoration offers the next best average service availability and expected loss in traffic even though it does not employ predefined restoration paths for protection.
3. Both dedicated protection and link restoration have very high average service availability, 0.999775872 and 0.999706856 respectively.

5.5 Simulation Results: Traffic Variation

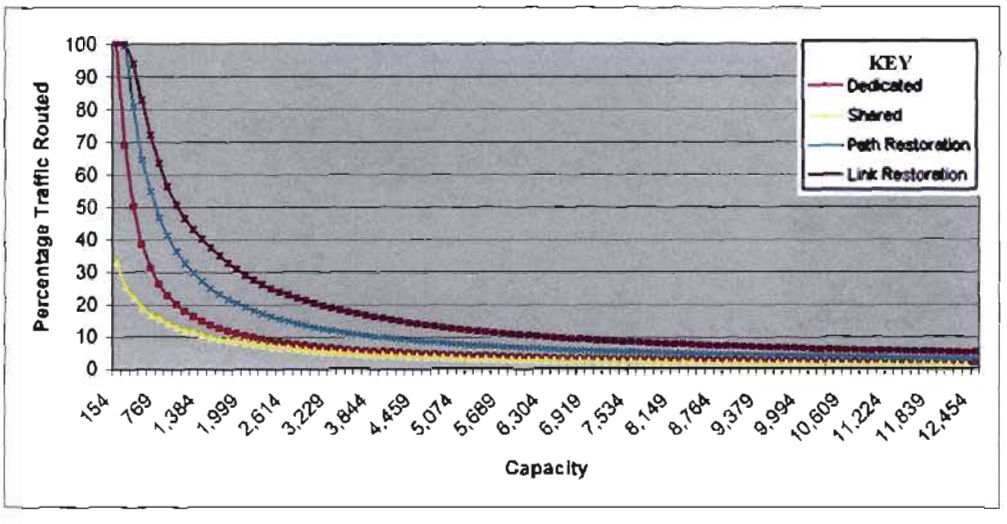
In this simulation scenario an in depth analysis of the network is carried out, in terms of the following parameters, percentage link and node utilization as well as percentage of traffic that was successfully routed for the various protection schemes after applying a random traffic increase to the network in Figure 5-1. The protections schemes are analysed as to how effective they are in handling projected traffic changes.



(a) 20% Traffic Increase



(b) 50% Traffic Increase



(c) 80% Traffic Increase

Figure 5-20 Percentage Traffic Routed for Percentage Traffic Increase

A random churn was used to simulate projected traffic increases of 20%, 40%, 50%, 60% and 80%. Each projected traffic increase was run for 100 iterations and the effects these increases had on traffic routed in the network was recorded. For illustration purposes we have only presented the results for 20%, 50% and 80% traffic increase. For a bigger view of the presented graphs as well as the results obtained for 40% and 60% traffic increases refer to Appendix DI and for the numerical results obtained for each percentage traffic increase refer to Appendix D1-1 on CD rom.

The graphs in Figure 5-20a, b and c represent a 20%, 50% and 80% traffic increase in the network respectively. From these plots the values indicated on the x axis denote the capacity in the network for a given percentage increase. The values on the y axis are indicative of the percentage of traffic routed that was routed successfully. From the plots one can ascertain which protection scheme best accommodates the increase in traffic.

5.5.1 Discussion of Results for Percentage Traffic Routed

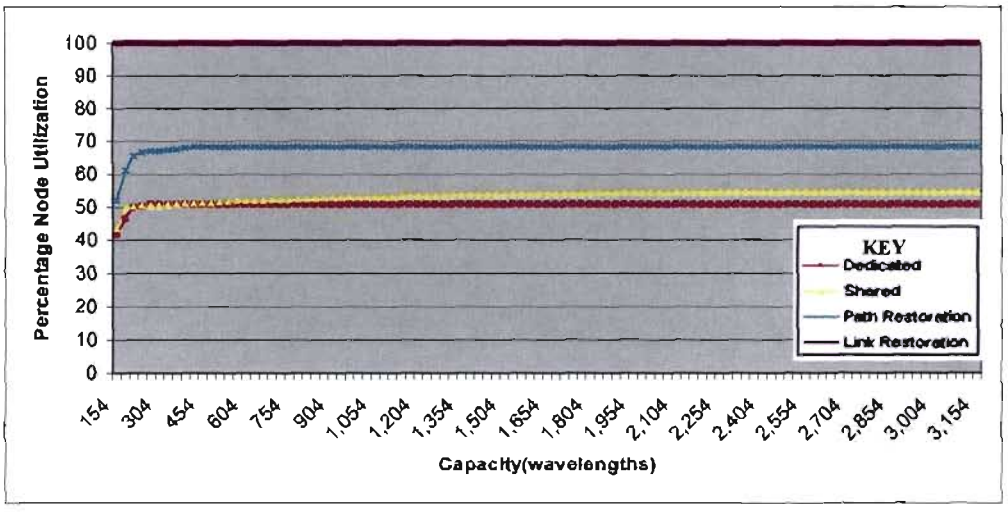
1. The first observation from the plots of the various traffic increases is that, as the traffic increases the slope of the protection scheme curves become very sharp. This simply implies that as the amount of traffic increases in the protection schemes become more taxed and as a result their performance in terms of percentage traffic routed deteriorates.

2. To illustrate this deterioration lets isolate one of the schemes and compare them graphically across all three plots in Figure 5-20. Choosing the yellow curve which corresponds to shared path protection, we observe that at 20% traffic increase approximately 45% of the traffic was successfully routed. At 50% traffic increase approximately 38% traffic was successfully routed and at 80% traffic increase approximately 32% of traffic was successfully routed.

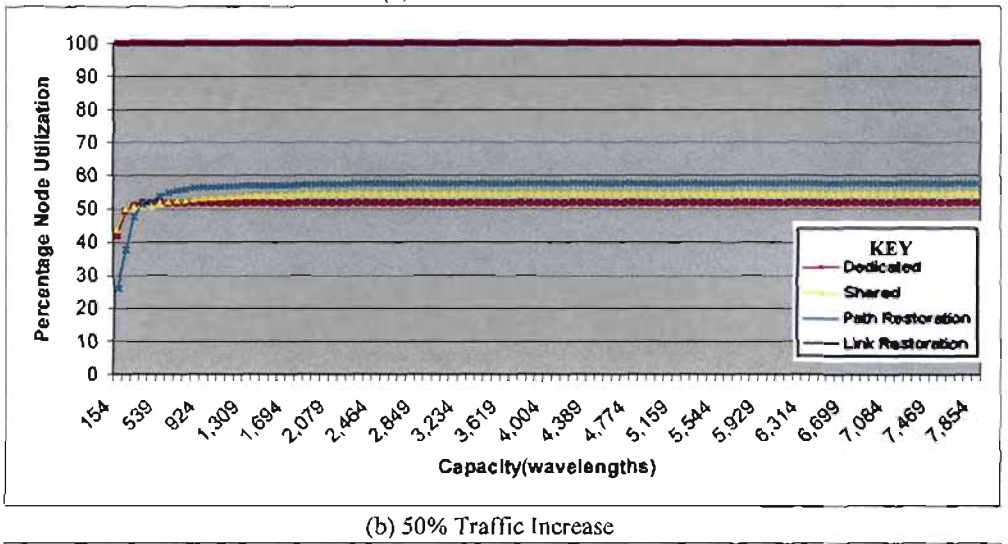
3. Path Restoration performs poorly with regards to routing of traffic at 20% traffic increase as can be seen from Figure 5-20a, however as the percentage traffic increases it performs better.

4. Link Utilization seems to be the better performer in terms of ability to route traffic successfully across all traffic increases. The other schemes offer mediocre performance as compared to link restoration, with shared path protection performing the worst.

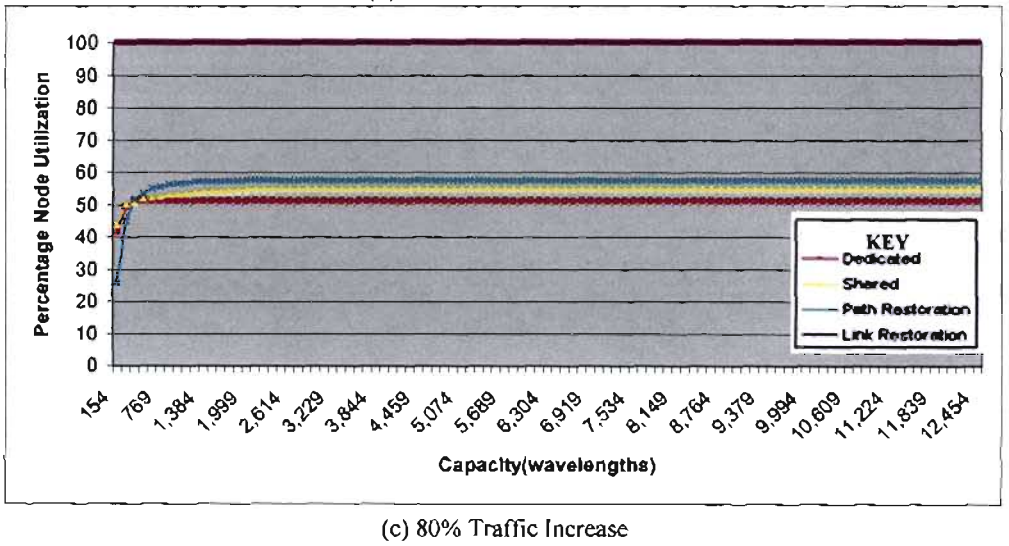
In Figure 5-21 that follows a similar type of comparison is done, but instead of looking at percentage traffic routed we now focus on percentage node utilization.



(a) 20% Traffic Increase



(b) 50% Traffic Increase



(c) 80% Traffic Increase

Figure 5-21 Percentage node utilization for percentage traffic increase.

A random churn was used to simulate projected traffic increases of 20%, 40%, 50%, 60% and 80%. Each projected traffic increase was run for 100 iterations and the effects these increases had on node utilization were recorded. Here again we only present the results for 20%, 50% and 80% traffic increase for illustration purposes. For a bigger view of the presented graphs as well as the results obtained for 40% and 60% traffic increases refer to Appendix D2 and for the numerical results obtained for each percentage traffic increase refer to Appendix D2-2 on CD rom.

The graphs in Figure 5-21a, b and c represent a 20%, 50% and 80% traffic increase in the network respectively. From these plots the values indicated on the x axis denote the capacity in the network for a given percentage increase. The values on the y axis are indicative of the percentage node utilization. From the plots one can ascertain what the node utilization is for a specific protection scheme and how this utilization is affected with increasing traffic. This is one of the crucial parameters to be analysed when designing survivable networks since node failures have the greatest impact on network traffic as compared to any other type of failure.

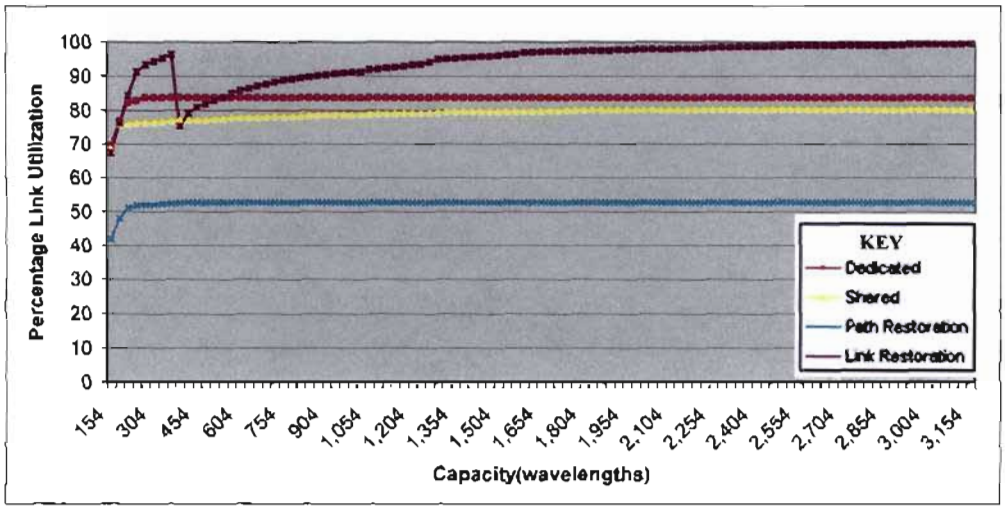
5.5.2 Discussion of Results for Percentage Node Utilization

1. The most prominent feature during the analysis of the results for node utilization under varying increases in traffic is that link restoration exhibits 100% node utilization for all traffic increases(refer to Appendix D2 for a clearer plot), hence from this we see that in order for link restoration to function it relies heavily on the nodes in the network.

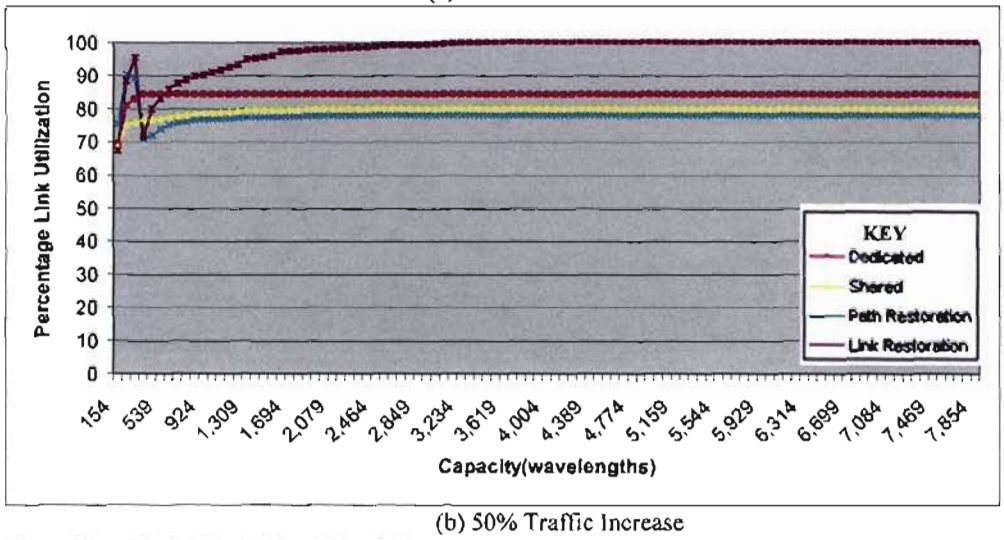
2. At low capacities dedicated and shared path protection exhibit similar node utilization with only a marginal difference between them as the capacity increases.

3. Node utilization for shared path protection is second highest in Figure 5-21a for 20% traffic increase but it drops drastically from 70% node utilization to almost 55% when there is a traffic increase above 50%.

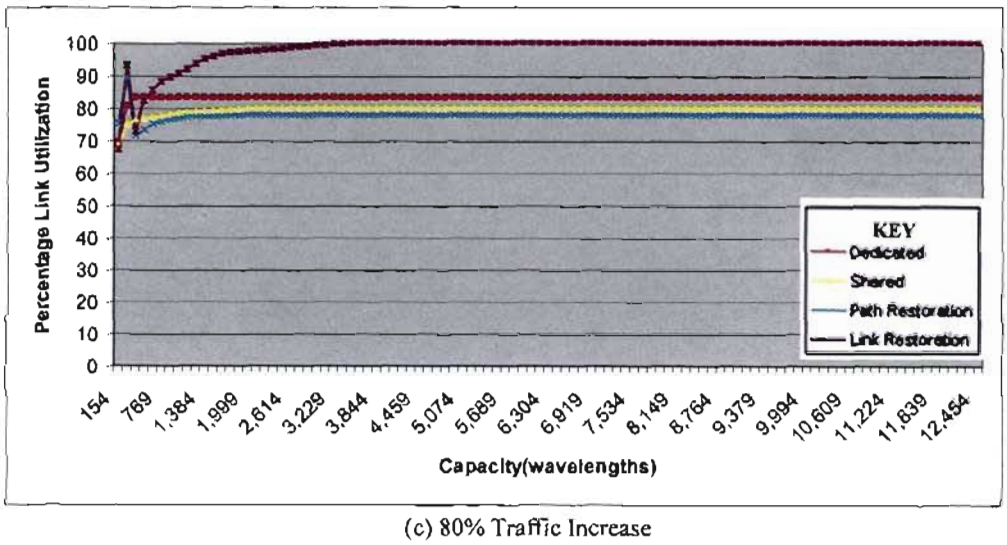
4. From the graphs in Figure 5-21, it is apparent that link restoration places the highest demand on the network in terms of node utilization, it is followed by path restoration, shared path protection and dedicated protection.



(a) 20% Traffic Increase



(b) 50% Traffic Increase



(c) 80% Traffic Increase

Figure 5- 22 Percentage Link Utilization for Percentage Traffic Increase

In the graphs presented in Figure 5-22 similar type of comparison is done, but instead of looking at percentage node utilization we now focus on percentage link utilization.

A random churn was used to simulate projected traffic increases of 20%, 40%, 50%, 60% and 80%. Each projected traffic increase was run for 100 iterations and the effects these increases had on link utilization were recorded. Here again we only present the results for 20%, 50% and 80% traffic increase for illustration purposes. For a bigger view of the presented graphs as well as the results obtained for 40% and 60% traffic increases refer to Appendix D3 and for the numerical results obtained for each percentage traffic increase refer to Appendix D3-3 on CD rom.

The graphs in Figure 5-22a, b and c represent a 20%, 50% and 80% traffic increase in the network respectively. From these plots the values indicated on the x axis denote the capacity in the network for a given percentage increase. The values on the y axis are indicative of the percentage link utilization. From the plots one can ascertain what the link utilization is for a specific protection scheme and how this utilization is affected with increasing traffic. This parameters is second to that of node utilization but still it plays a fundamental role when designing survivable networks since links are the media on which traffic is transmitted on and failures will directly impact on the survivability of the network.

5.5.3 Discussion of Results for Percentage Link Utilization

Link restoration also approaches 100% link utilization for all projected traffic increases, however its behaviour at low capacities is erratic and its approach to 100% link utilization is gradual see Appendix D3 for clearer plot of percentage link utilization.

From the graphs in Figure 5-22 dedicated and shared path protection have almost a 84% and 80 % link utilization respectively, these high percentage utilizations are attributed to these schemes using predetermined paths for routing.

Path restoration exhibits very low link utilization at low projected traffic increases as illustrated in Figure 5-22a, however as the percentage traffic increases its link utilization at low capacity is almost like link restoration but as the capacity increases the percentage link

utilization for path restoration then follows the pattern of dedicated and shared path protection.

Chapter 6

Conclusion and Recommendations

6.1 Conclusions

The aim of this research was to investigate survivability strategies in Optical Networks, this could only be achieved once a proper knowledge of the operations involved in optical networking was understood hence a extensive literature survey was done. From the many survivability strategies that can be employed in Optical Networks, it was decided to focus our investigation on the mechanism of protection as a survivability strategy.

From the simulation results presented in Chapter 5, the following conclusions regarding the performance of the various types of protection schemes for node and link failure can be made. In terms of the number of wavelengths affected by link failures, a comparative analysis of all the protection schemes revealed that dedicated and shared path protection had the most adverse effects as shown in Figure 5-8, since even at low percentage failures more wavelengths were affected by these schemes than path and link restoration. When considering the number of wavelengths that were recovered for the link failure scenarios, Figure 5-9 showed dedicated and shared protection exhibited better recovery at percentage failures slightly lower than 25%, however link restoration out performed all schemes in terms of number of wavelengths recovered when analysed from 25%-70% link failures.

For the node failure scenarios, the total number of wavelengths affected by the varying percentage node failures seemed to be more or less consistent for all the protection schemes as can be seen from Figure 5-16 with slightly greater number of wavelengths being affected by dedicated protection and shared path protection. This fractional increase could be attributed to the fact that these protection schemes use predetermined backup paths to achieve protection. In terms of wavelength recovery dedicated and shared path protection perform well at node failures below 15%, however at percentage

node failures from 15%-70% path restoration exhibits the best wavelength recovery. A very striking observation of wavelength recovery, is that Link Restoration scheme which performed so well for link failures scenario exhibited the worst performance for the node failure scenarios since it was unable to recover any wavelengths as depicted by Figure 5-17.

The results obtained for link availability analysis shows that Dedicated Path Protection exhibits the best average service availability, this is a desirable quality since most SLA's require high service availability. Dedicated Protection offers the next highest average service availability followed by Link Restoration, Path Restoration and Shared Path Protection as shown in Figure 5-18. In terms of expected loss in traffic, Unprotected scenario yielded a extremely high loss of traffic as compared to the rest of the protection schemes, this observation proves that having a protection scheme in place will definitely go a long way in ensuring that traffic loss is kept to a minimum. In this simulation scenario dedicated protection again exhibited lowest loss in traffic, followed closely by Link Restoration as seen in Figure 5-19.

Traffic variations are common in any network, the simulations to determine the percentage traffic routed revealed how the increased traffic affected this routing for each protection scheme. When comparing the results in Figure 5-20 the most apparent observation is that as the traffic increases the percentage traffic routed decreases. This follows since an increase in traffic implies a strain on network resources. Link Restoration exhibits the highest percentage of traffic routed for all percentage traffic increases followed by Path Restoration. The other schemes perform poorly by comparison.

Another parameter that is observed when traffic is increased is percentage node utilization. In terms of node utilization Figure 5-21 shows the dependency that Link Restoration has on nodes in the network. Link Restoration has a 100% node utilization for traffic increases from 20%-80%. This result substantiates the poor performance Link Restoration exhibited in the node failure scenarios, due to its dependence on nodes to

implement protection effectively Link Restoration cannot function efficiently when nodes in a network fail.

The next parameter that was observed was percentage link utilization. Here as well the percentage link utilization for Link Restoration is erratic at low capacities but it then approaches 100%. Dedicated and Shared Path protection exhibit high link utilization as well, having 84% and 80% link utilization respectively. For increased traffic patterns Path Restoration behaves much like Link restoration at low capacity but as capacity increase it follows a pattern similar to Dedicated and Shared Path Protection having a lower percentage link utilization overall.

6.2 Recommendations

- From the simulations it is apparent that Link Restoration performs the best for link failure and should be used when link failures in a network exceed 25%.
- In terms of node failure Path Restoration should be used as protection for node failures exceeding 15%.
- Link Restoration should not be used if nodes in a network are failing since it offers no protection to node failures.
- A better alternative for protection at high percentage failures is path restoration which performs fairly well in both link and node failures
- For low percentage of failures Dedicated Protection performs well but the trade off is high link utilization.
- Depending on the Service Level Agreement, the designer can choose to have a high degree of average service availability offered by dedicated protection but run the risk of also taxing network resources unnecessarily.

On average path restoration seems to be exhibiting good performance values to make it a primary contender for being implemented as a survivability mechanism that will ensure that from all the protection schemes it delivers the best protection. Prior knowledge of the networks failure history will help in choosing a suitable protection scheme.

6.3 Future Work

In this work we have only examined protection as a means of achieving survivability in optical networks. Further work can be conducted in terms of wavelength assignment and routing, since these two go hand in hand and are critical to ensuring that the network is functioning optimally. A number of routing and assignment algorithms are already in existence but the way in which they can be tied to ensuring that survivability mechanism such as protection schemes function optimally, needs to be investigated.

References

[1] R. Ramaswamy and K. N. Sivarajan, Routing and wavelength assignment in all-optical networks," IEEE/ACM Transactions on Networking, volume 3, no 5, pp 489-500, October 1995.

[2] E. Leonardi, M. Mellia and M. A. Marsan, "Algorithms for the logical topology design in WDM all-optical networks" Optical Networks Magazine, volume 1, pp 35-46, January 2000.

[3] Paul Bonenfant and Antonio Rodriguez-Moral. Optical data networking, IEEE Communications Magazine, pp 63–70, February 2000.

[4] B. V. Caenegem, W. V. Parys, F. De Turck, and P. M. Demeester, Dimensioning of survivable WDM networks," IEEE Journal of Selected Areas in Communications, volume16, no. 7, pp 1146-1157, September 1998.

[5] O. Crochat and J. Y. Boudec, Design protection for wdm optical networks, IEEE Journal of Selected Areas in Communications, volume 16, no. 7, pp 1158-1165, September 1998.

[6] Y. Miyao and H. Saito, Optimal design and evaluation of survivable wdm transport networks," IEEE Journal of Selected Areas in Communications, volume 16, no 7, pp 1190-1198, September 1998.

[7] R. Ramaswami and K. N. Sivarajan, Optical Networks: A Practical Perspective, Morgan Kaufmann, San Francisco, CA 1998.

[8] L. Ruan and D. Z Du, Optical Networks: Recent Advances, Kluwer Academic Publishers, Netherlands, 2001.

[9] U. Black, Optical Networks 3rd Generation Transport Systems, Prentice Hall, New Jersey, 2002.

[10] I. Chlamtac, A. Ganz and G. Karmi, Lightpath Communications : An Approach to High Bandwidth Optical WAN's," IEEE Transaction on Communication, vol. 40, pp 1171-1182, July 1992.

[11] I. Chlamtac, A. Ganz and G. Karmi, Purely Optical Networks for Terabit Communication," IEEE, INFOCOM, 1989.

[12] E. Karasan and E. Ayanoglu, Effects of Wavelength Routing and Selection Algorithms on Wavelength Conversion Gain in WDM Optical Net-works," IEEE/ACM Transaction on Networking, vol. 6, no. 2, pp 186-196, Apr. 1998.

[13] R. A. Barry and P. A. Humblet, "Models of blocking probability in all optical networks with and without wavelength changers," in Proc. IEEE INFOCOM'95, Boston, MA, April 1995, pp 402-412.

[14] R. A. Barry and D. Marquis, "Evaluation of a model of blocking probability in all-optical mesh networks without wavelength changers," in Proc. SPIE Photonics East, Philadelphia, PA, October 1995, pp 154-163.

[15] A. Girard, "Routing and Dimensioning in Circuit-Switched Networks", MA: Addison-Wesley, 1990.

[16] J. Y. Hui, "Switching and Traffic Theory for Integrated Broadband Networks", Norwood, MA: Kluwer, 1990.

[17] R. A. Barry and D. Marquis, "An improved model of blocking probability in all-optical networks," in Dig. LEOS Summer Topical Meetings, Keystone, CO, August 1995, pp 43-44.

[19] G. Jeong and E. Ayanoglu, "Comparison of wavelength-interchanging and wavelength-selective cross-connects in multi wavelength all-optical networks," in Proc. IEEE INFOCOM'96, San Francisco, CA, March 1996, pp 156-163.

[20] D. Bertsekas and R. Gallager, Data Networks, New Jersey, Prentice-Hall, 1992.

[21] J. Y. Hui, "Switching and Traffic Theory for Integrated Broadband Networks. Norwood, MA: Kluwer, 1990.

[22] K. Bala Tellium Whitepaper, WDM Optical Network Architectures for Data Centric Environment.

[23] P. Tomsu, Next Generation Optical Networks: The Convergence of IP Intelligence and Optical Technologies, Prentice Hall, 2002

[24] A. Fumagalli and L. Valcarenghi, "Ip Restoration versus WDM Protection: Is there an Optimal Choice?", IEEE Network Magazine-Optical Communication Networks for the Next-Generation Internet, vol. 14, no. 6, pp 34-41 November 2000.

[25] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part 1-Protection", IEEE INFOCOM '99, New York, pp 744-751, March 1999.

[26] P.H. Ho and T.M. Hussein, "A framework for service-guaranteed shared protection in WDM mesh networks", IEEE Communication Magazine, pp 97-103, February 2002.

[27] M. R.Wilson, "The Quantitative Impact of Survivable Network Architectures on Service Availability," IEEE Communications Magazine, May 1998.

[28] K. Murakami, H.S. Kim, "Comparative Study on Restoration Schemes of Survivable ATM Networks," IEEE INFOCOM 1997, Kobe, Japan, April 1997.

[29] Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part 2-Restoration", IEEE ICC '99, Vancouver, pp 23-30, June 1999.

[30] C.Siva a.d G.Mohan, "WDM Optical Networks: Concepts, Design and Algorithms". Prentice Hall, New Jersey, USA, November 2001.

[31] S.Gowda and K.M. Sivalingam, Protection Mechanisms for Optical WDM Networks based on Wavelength Converter Multiplexing and Backup Path Relocation Techniques, IEEE INFOCOM, 2003.

[32] E. Modlano and P.J. Lin, Traffic Grooming in WDM Networks, IEEE Communications Magazine, July 2001.

[33] B. Mukhurjee, Optical Communication Networks, McGraw-Hill Publishers, 1997.

[34] T.E. Stern and K.Bala, Multiwavelength Optical Networks, Addison Wesley Publishers, 1999.

[35] I. Chlamtac, A. Farago and T.Zhang, Lightpath Routing in Large WDM Networks, IEEE Journal Selected Areas in Communication, Vol.14 No.5, pp 909-913, 1995.

[36] A. Sridharan and K.N. Sivarajan, "Blocking in All-Optical Networks", IEEE INFOCOM, pp 990-999, 2000.

[37] E.Boulillet and J.F Labourdette, Distributed Computation of Shared Backup Path in Mesh Optical Networks Using Probabilistic Methods, IEEE/ACM Transactions, pp 920-930, October 2004.

[38] P.H Ho, J. Tapolcai and T. Cinkler, Segment Shared Protection in Mesh Communications Networks with Bandwidth Guaranteed Tunnels, IEEE/ACM Transactions, pp 1105-1118.

[39] K.Lu, G. Xiao, Analysis of Blocking Probability for Distributed Lightpath Establishment in WDM Optical Networks, IEEE/ACM Transactions, pp187-197, February 2005.

[40] X.Chu, B. Li, Dynamic Routing and Wavelength Assignment in Presence of Wavelength Conversion for All-Optical Networks, IEEE/ACM Transactions, pp704-714, June 2005.

[41] P. Saengudomlert, E.H. Modiano and R.G. Gallager, Dynamic Wavelength Assignment for WDM All-Optical Tree Networks, IEEE/ACM Transactions, pp 895-905, August 2005.

[42] L. Shen, X.Yang and Byrav Ramamurthy, Shared Risk Link Group-Diverse Path Provisioning Under Hybrid Service Level Agreements in Wavelength-Routed Optical Mesh Networks, IEEE/ACM Transactions, pp 918-931, August 2005.

[43] http://www.bel-labs.com/project/MONET

[44] http://www.tek.com/Measurement/App%20Notes/SONET/

[45] http://www.ece.umn.edu/users/rsgt/papers/globecom2001.pdf

[46] http://www.eurescom.de/~public-seminars/1998/OADM/Proceedings/Paper16.html

[47] http://www.networkworld.com/edge/research/optical.html

[48] http://www.sprintlabs.com/~ashwin/papers/opt_blocking.pdf

[49] http://dawn.cs.umbc.edu/Slides/WDM-Mahesh-Sep02.ppt#256

[50] http://www.itss.brockport.edu/~vanand/rep1.htm

[51] http://www4.ncsu.edu:8030/~rouskas/Ar0ra/Books/Networking-Rouskas-2002.pdf

[52] http://www.eurescom.de/~public-seminars/1998/OADM/Proceedings/Paper16.html

[53] http://www.lucent.com/

[54] http://www.itu.int/ITU-T/studygroups/com15/otn/definitions.html

[55] http://www.cisco.com/univercd/cc/td/doc/product/mels/15540/planning/mpg_topo.htm

[56] http://www.osa.org/

Appendix A-1

Link Characteristics

From	To	Link Characteristics				
		Link Length (km)	Delay(ms)	Regen. Stations	OA Stations	Total Fiber Pairs
ATLANTA	MIAMI	961.93	4.810	1	8	50
ATLANTA	WASHINGTON	880.546	4.403	1	7	50
CHICAGO	ATLANTA	958.587	4.793	1	8	50
CHICAGO	DETROIT	385.554	1.928	0	3	50
DALLAS	ATLANTA	1158.63	5.793	1	10	50
DALLAS	CHICAGO	1292.95	6.465	2	10	50
DALLAS	HOUSTON	351.163	1.756	0	3	50
DETROIT	BOSTON	984.396	4.922	1	8	50
DETROIT	WASHINGTON	642.469	3.212	1	5	50
HOUSTON	ATLANTA	1110.36	5.552	1	10	50
HOUSTON	MIAMI	1553.41	7.767	2	13	50
HOUSTON	SAN_DIEGO	2092.97	10.465	3	17	50
LAS_VEGAS	DALLAS	1716.38	8.582	2	15	50
LOS_ANGELES	LAS_VEGAS	359.498	1.797	0	3	50
LOS_ANGELES	SAN_DIEGO	176.913	0.885	0	1	50
LOS_ANGELES	SAN_FRAN	560.733	2.804	0	5	50
NEW_YORK	BOSTON	301.199	1.506	0	3	50
SAN_DIEGO	LAS_VEGAS	415.665	2.078	0	4	50
SAN_FRAN	LAS_VEGAS	672.993	3.365	1	5	50
SEATTLE	CHICAGO	2789.03	13.945	4	23	50
SEATTLE	LAS_VEGAS	1415.35	7.077	2	12	50
SEATTLE	SAN_FRAN	1100.23	5.501	1	10	50
WASHINGTON	NEW_YORK	339.172	1.696	0	3	50

Table A-1 Link Browser Table

Table provides information regarding the following physical characteristic of the network model used for simulations in chapter 5:-

Link Length - Length of fiber between nodes

Delay – Delay experienced by particular fiber

Regen.Stations - Number of regeneration stations on that particular link

OA Stations - Number of optical amplifier stations on each link

Total Fiber Pairs - Total number of fiber pairs available on each link

Appendix B-1

Link Failure Models

10% Link Failure

Cables Failed 10%

1) Cable LOS_ANGELES <-> SAN_DIEGO

2) Cable SEATTLE <-> CHICAGO

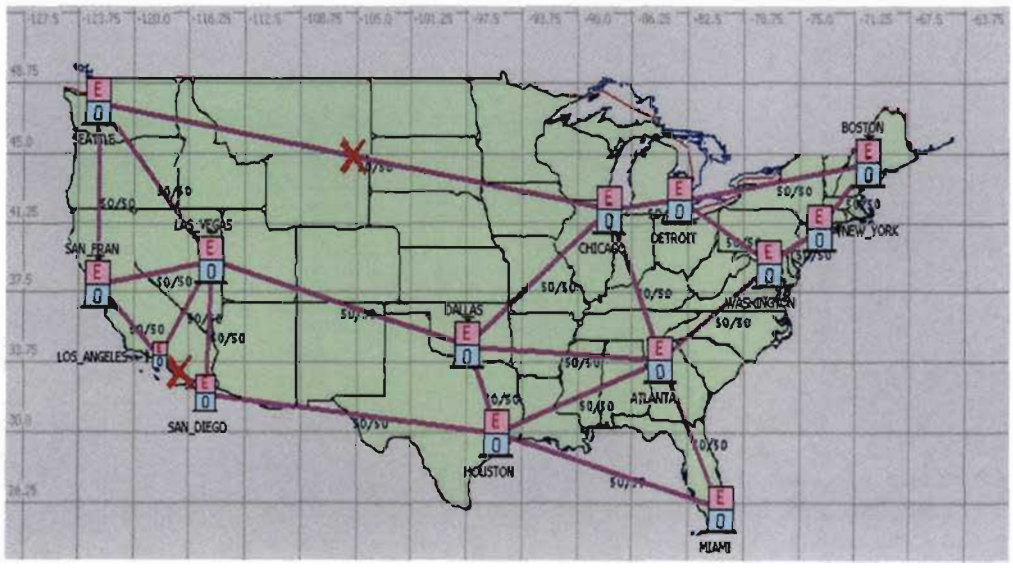


Figure B1-1 Model for 10% Link Failure

20% Link Failure

Cables Failed 20%

1) Cable LOS_ANGELES <-> SAN_DIEGO
2) Cable SEATTLE <-> CHICAGO
3) Cable SEATTLE <-> SAN_FRAN
4) Cable HOUSTON <-> SAN_DIEGO
5) Cable DETROIT <-> WASHINGTON

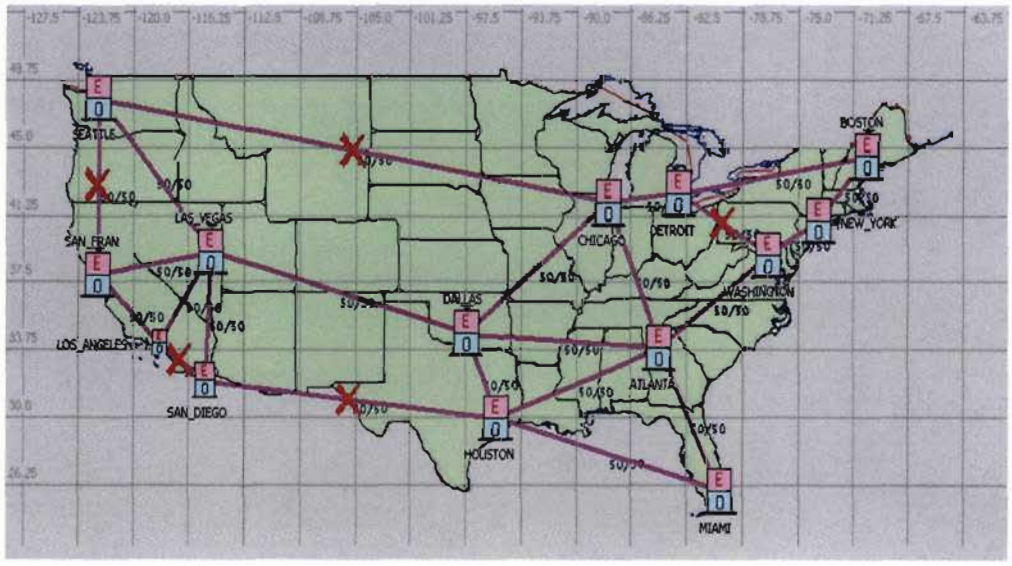


Figure B1-2 Model for 20% Link Failure

30% Link Failure

Cables Failed 30%

1) Cable SEATTLE <-> CHICAGO
2) Cable LOS_ANGELES <-> SAN_DIEGO
3) Cable SEATTLE <-> SAN_FRAN
4) Cable HOUSTON <-> SAN_DIEGO
5) Cable DETROIT <-> WASHINGTON
6) Cable DALLAS <-> CHICAGO
7) Cable LOS_ANGELES <-> SAN_FRAN

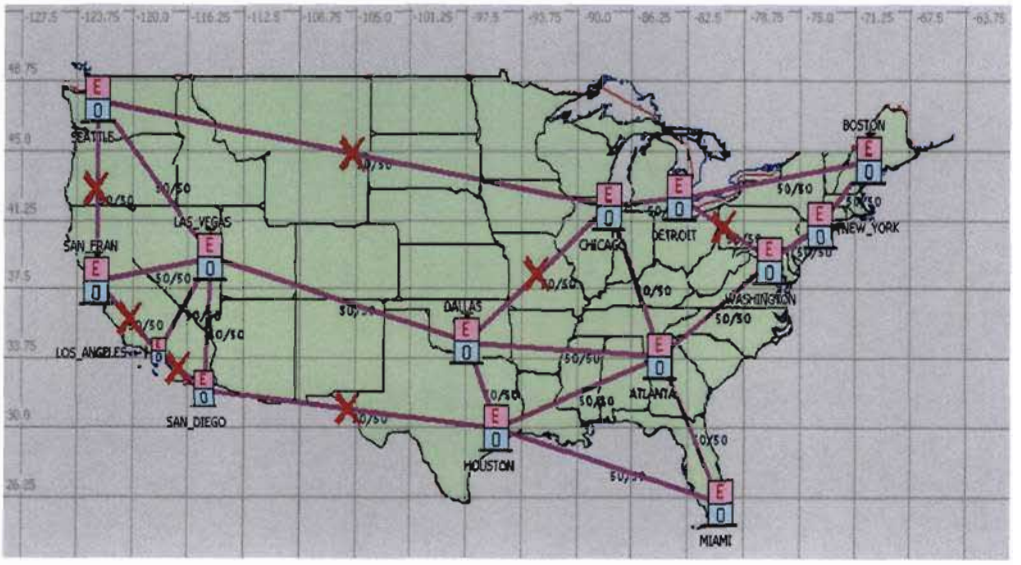


Figure B1-3 Model for 30% Link Failure

40% Link Failure

Cables Failed 40%

1) Cable SEATTLE <-> CHICAGO

2) Cable LOS_ANGELES <-> SAN_DIEGO

3) Cable SEATTLE <-> SAN_FRAN

4) Cable HOUSTON <-> SAN_DIEGO

5) Cable DETROIT <-> WASHINGTON

6) Cable DALLAS <-> CHICAGO

7) Cable LOS_ANGELES <-> SAN_FRAN

8) Cable NEW_YORK <-> BOSTON

9) Cable HOUSTON <-> MIAMI

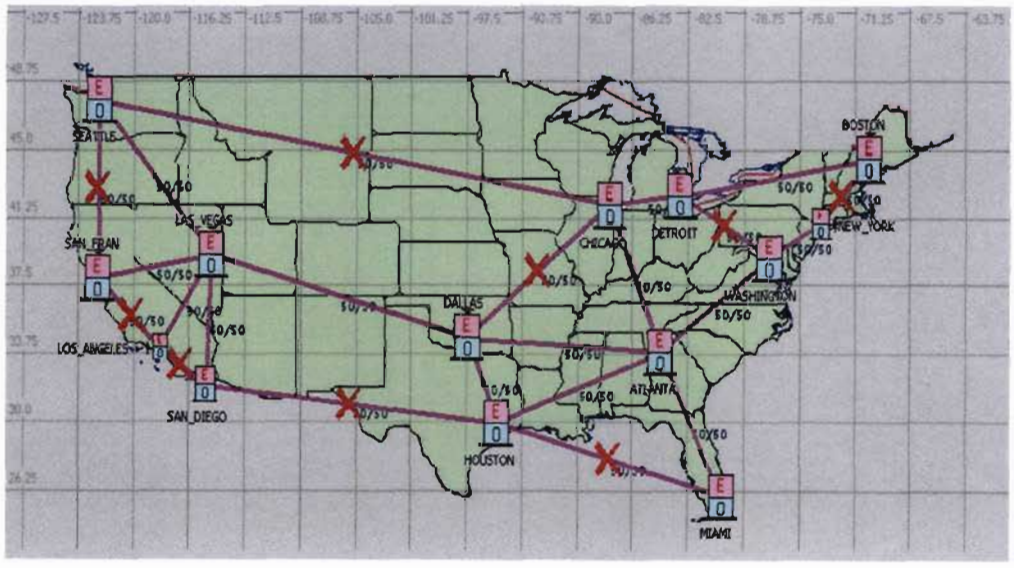


Figure B1-4 Model for 40% Link Failure

50% Link Failure

Cables Failed 50%

1) Cable LOS_ANGELES <->
SAN_DIEGO

2) Cable SEATTLE <-> CHICAGO

3) Cable SEATTLE <-> SAN_FRAN

4) Cable HOUSTON <-> SAN_DIEGO

5) Cable DETROIT <-> WASHINGTON

6) Cable LOS_ANGELES <-> SAN_FRAN

7) Cable DALLAS <-> CHICAGO

8) Cable HOUSTON <-> MIAMI

9) Cable NEW_YORK <-> BOSTON

10) Cable HOUSTON <-> ATLANTA

11) Cable DETROIT <-> BOSTON

12) Cable LOS_ANGELES <->
LAS_VEGAS

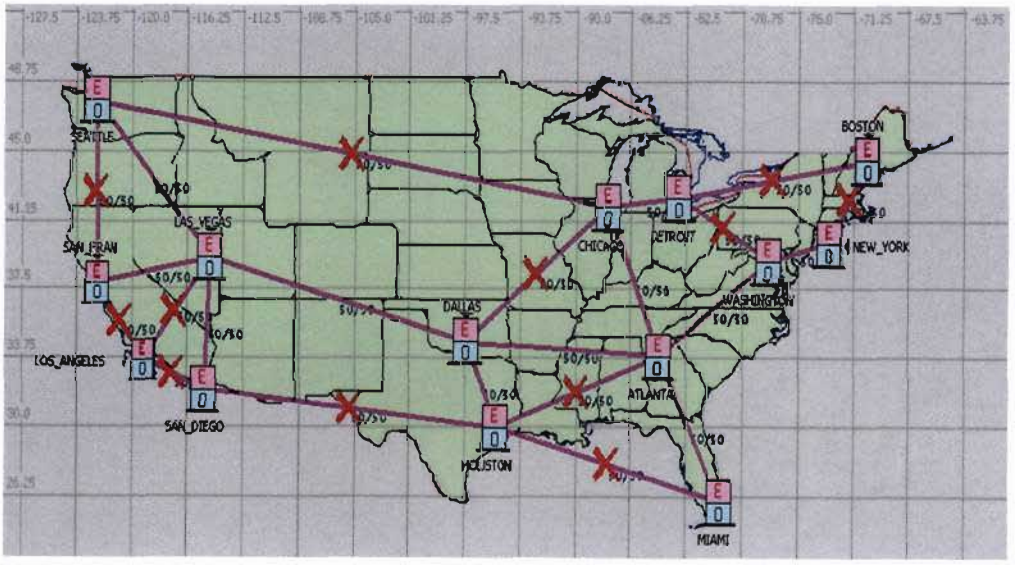


Figure B1-5 Model for 50% Link Failure

60% Failure

Cables Failed 60%

1) Cable SEATTLE <-> CHICAGO
2) Cable LOS_ANGELES <-> SAN_DIEGO
3) Cable SEATTLE <-> SAN_FRAN
4) Cable HOUSTON <-> SAN_DIEGO
5) Cable DETROIT <-> WASHINGTON
6) Cable LOS_ANGELES <-> SAN_FRAN
7) Cable DALLAS <-> CHICAGO
8) Cable NEW_YORK <-> BOSTON
9) Cable HOUSTON <-> MIAMI
10) Cable HOUSTON <-> ATLANTA
11) Cable DETROIT <-> BOSTON
12) Cable LOS_ANGELES <-> LAS_VEGAS
13) Cable SAN_FRAN <-> LAS_VEGAS
14) Cable ATLANTA <-> WASHINGTON

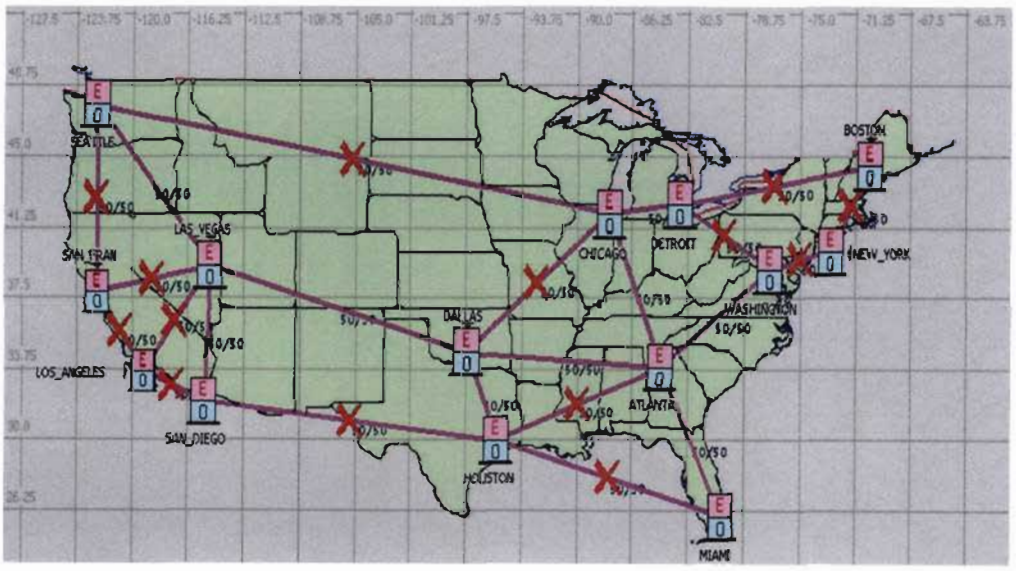


Figure B1-6 Model for 60% Link Failure

70% Link Failure

Cables Failed 70%

1) Cable LOS_ANGELES <-> SAN_DIEGO
2) Cable SEATTLE <-> CHICAGO
3) Cable SEATTLE <-> SAN_FRAN
4) Cable HOUSTON <-> SAN_DIEGO
5) Cable DETROIT <-> WASHINGTON
6) Cable LOS_ANGELES <-> SAN_FRAN
7) Cable DALLAS <-> CHICAGO
8) Cable HOUSTON <-> MIAMI
9) Cable NEW_YORK <-> BOSTON
10) Cable HOUSTON <-> ATLANTA
11) Cable DETROIT <-> BOSTON
12) Cable LOS_ANGELES <-> LAS_VEGAS
13) Cable SAN_FRAN <-> LAS_VEGAS
14) Cable ATLANTA <-> WASHINGTON
15) Cable DALLAS <-> ATLANTA
16) Cable SAN_DIEGO <-> LAS_VEGAS

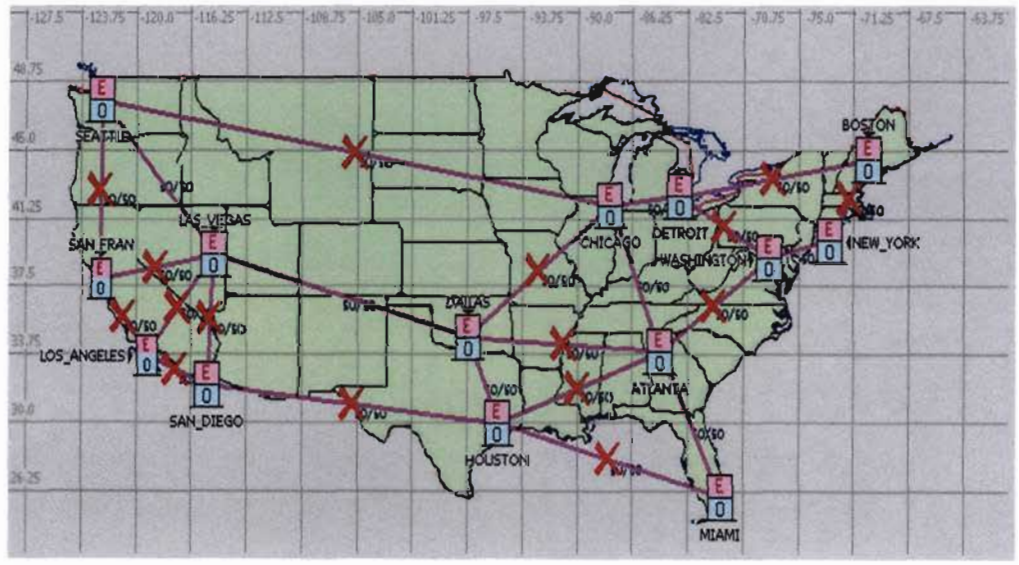


Figure B1-7 Model for 70% Link Failure

80% Link Failure

Cables Failed 80%

1) Cable LOS_ANGELES <-> SAN_DIEGO
2) Cable SEATTLE <-> CHICAGO
3) Cable SEATTLE <-> SAN_FRAN
4) Cable HOUSTON <-> SAN_DIEGO
5) Cable DETROIT <-> WASHINGTON
6) Cable LOS_ANGELES <-> SAN_FRAN
7) Cable DALLAS <-> CHICAGO
8) Cable HOUSTON <-> MIAMI
9) Cable NEW_YORK <-> BOSTON
10) Cable HOUSTON <-> ATLANTA
11) Cable DETROIT <-> BOSTON
12) Cable LOS_ANGELES <-> LAS_VEGAS
13) Cable SAN_FRAN <-> LAS_VEGAS
14) Cable ATLANTA <-> WASHINGTON
15) Cable DALLAS <-> ATLANTA
16) Cable SAN_DIEGO <-> LAS_VEGAS
17) Cable SEATTLE <-> LAS_VEGAS
18) Cable WASHINGTON <-> NEW_YORK

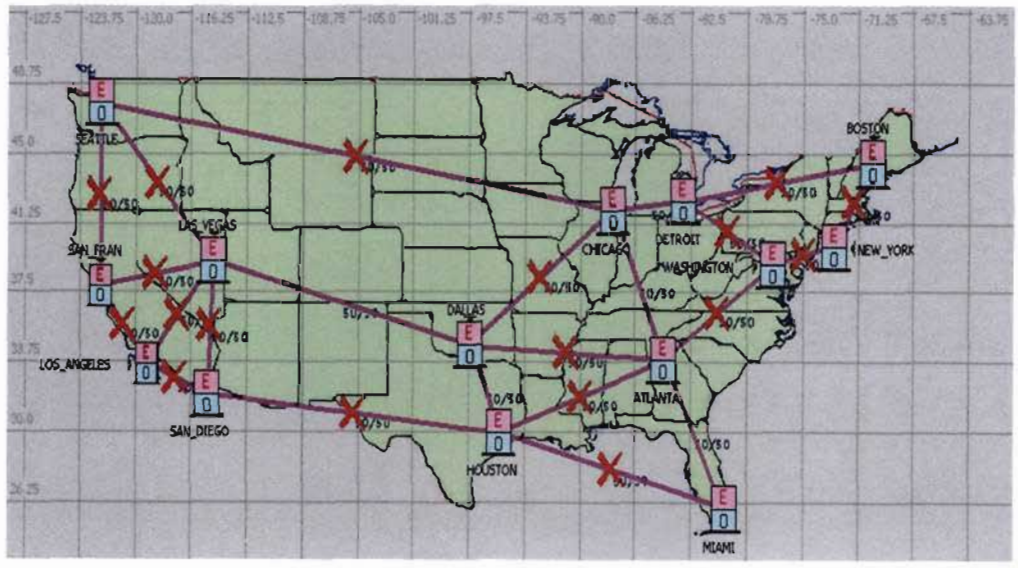


Figure B1-8 Model for 80% Link Failure

Appendix C-1

Node Failure Models

10% Node Failure

Nodes Failed 10%

1) Node SEATTLE (OTS)

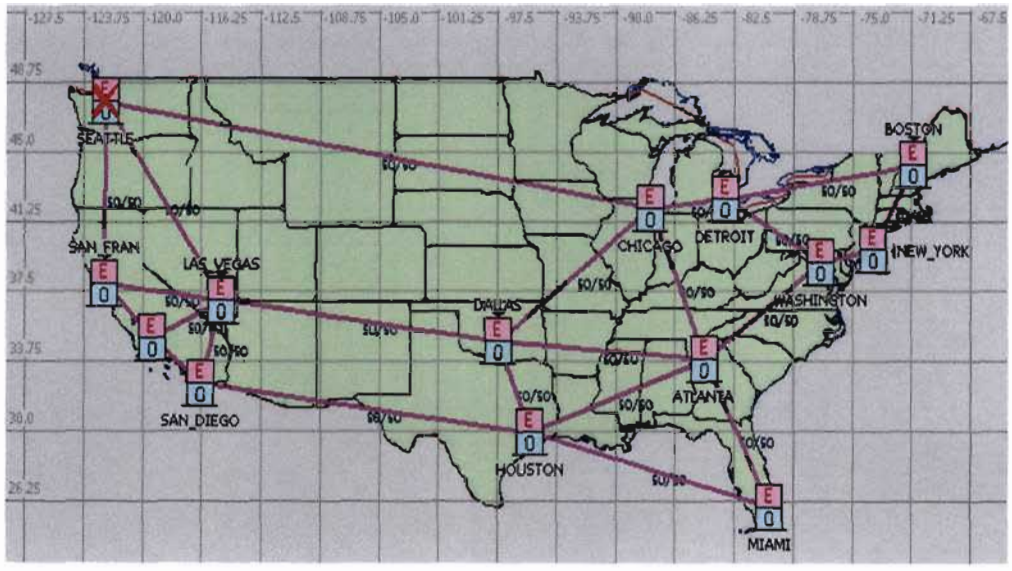


Figure C1-1 Model for 10% Node Failure

20% Node Failure

Nodes Failed 20%

1) Node SEATTLE (OTS)

2) Node DALLAS (OTS)

3) Node BOSTON (OTS)

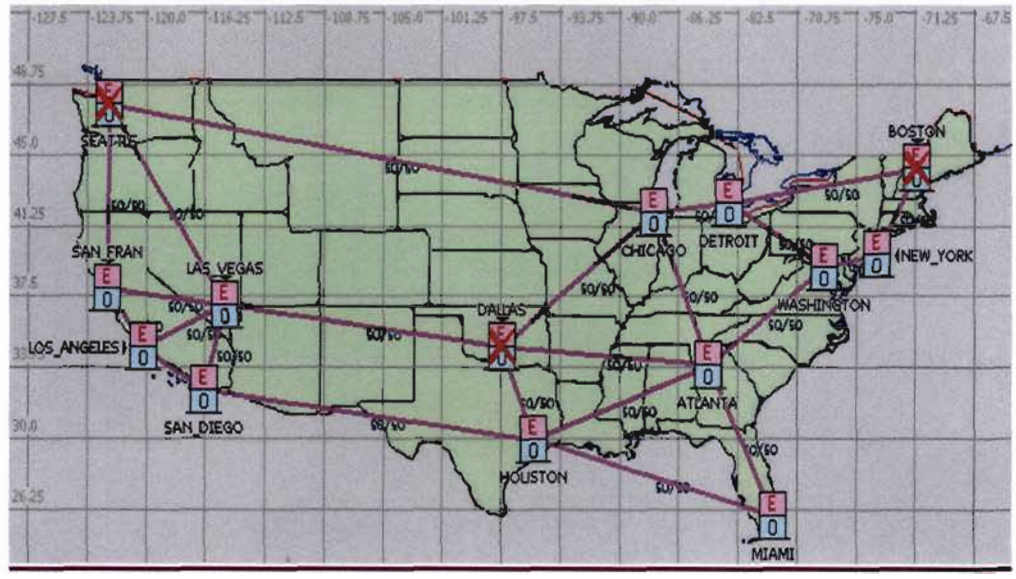


Figure C1-2 Model for 20% Node Failure

30% Node Failure

Nodes Failed 30%

1) Node SEATTLE (OTS)

2) Node DALLAS (OTS)

3) Node BOSTON (OTS)

4) Node LOS_ANGELES (OTS)

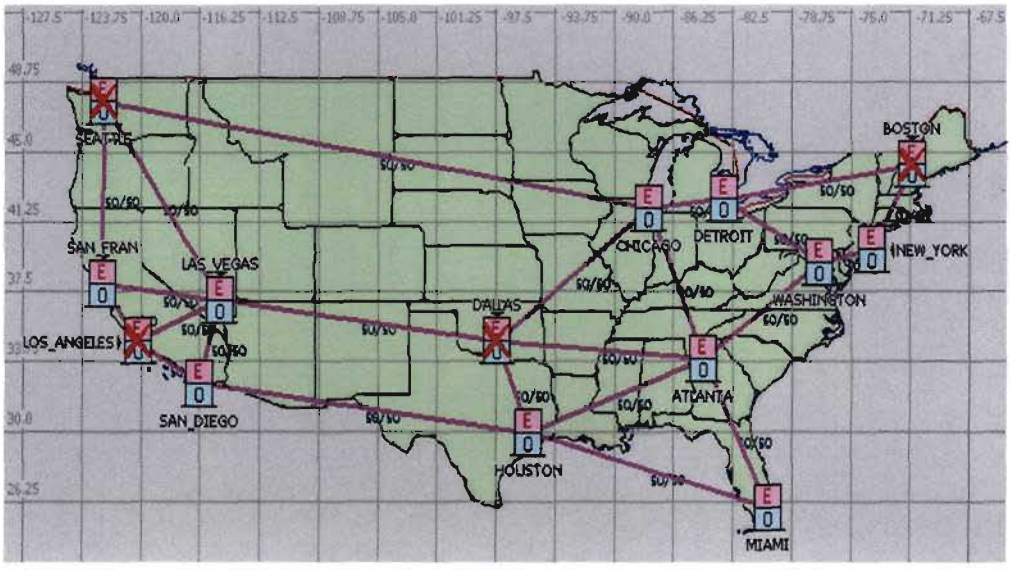


Figure C1-3 Model for 30% Node Failure

40% Node Failure

Nodes Failed 40%

1) Node SEATTLE (OTS)

2) Node DALLAS (OTS)

3) Node BOSTON (OTS)

4) Node LOS_ANGELES (OTS)

5) Node MIAMI (OTS)

6) Node CHICAGO (OTS)

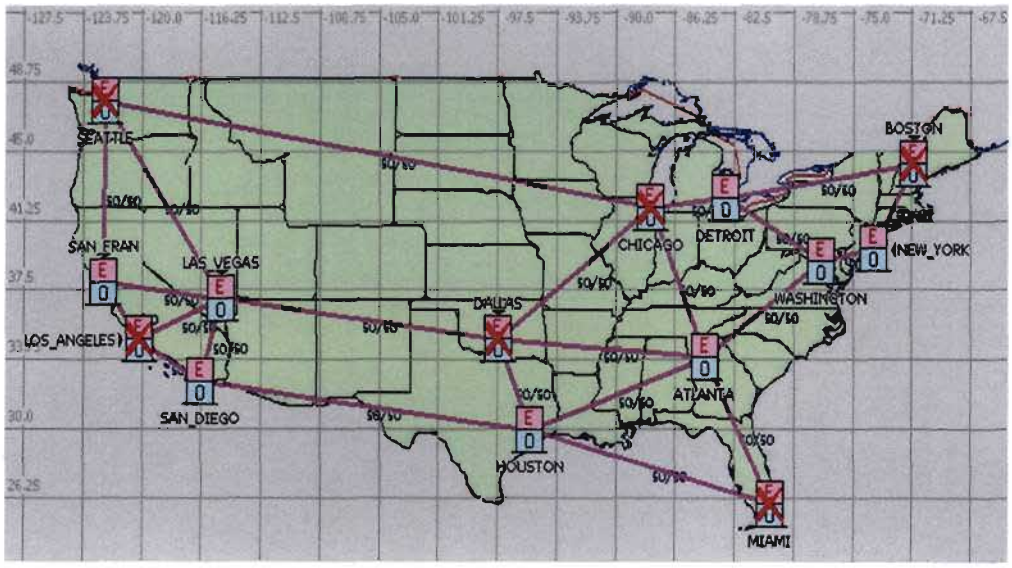


Figure C1-4 Model for 40% Node Failure

50% Node Failure

Nodes Failed 50%

1) Node SEATTLE (OTS)
2) Node DALLAS (OTS)
3) Node BOSTON (OTS)
4) Node LOS_ANGELES (OTS)
5) Node MIAMI (OTS)
6) Node CHICAGO (OTS)
7) Node WASHINGTON (OTS)

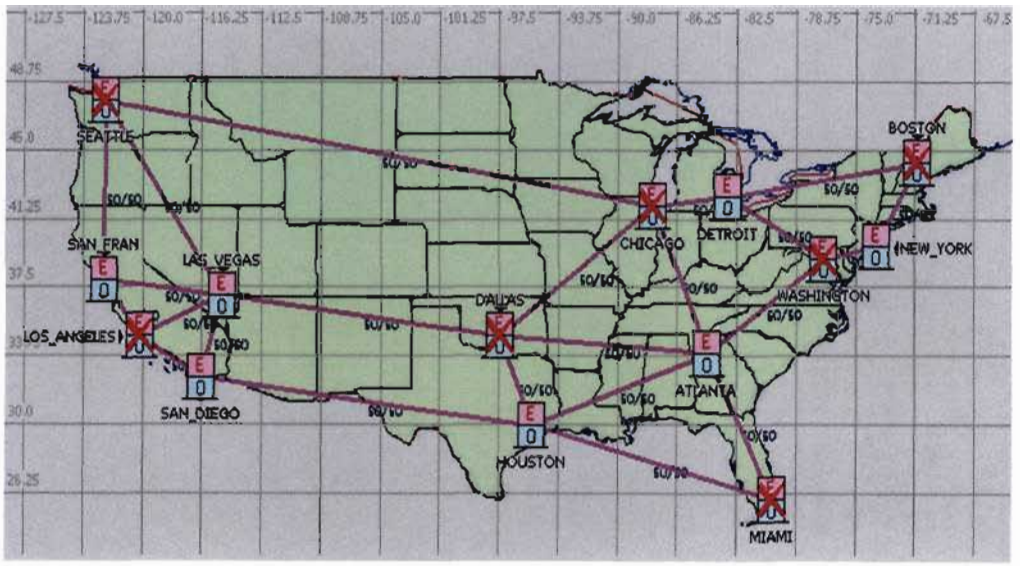


Figure C1-5 Model for 50% Node Failure

60% Node Failure

Nodes Failed 60%

1) Node SEATTLE (OTS)
2) Node DALLAS (OTS)
3) Node BOSTON (OTS)
4) Node LOS_ANGELES (OTS)
5) Node MIAMI (OTS)
6) Node CHICAGO (OTS)
7) Node WASHINGTON (OTS)
8) Node ATLANTA (OTS)

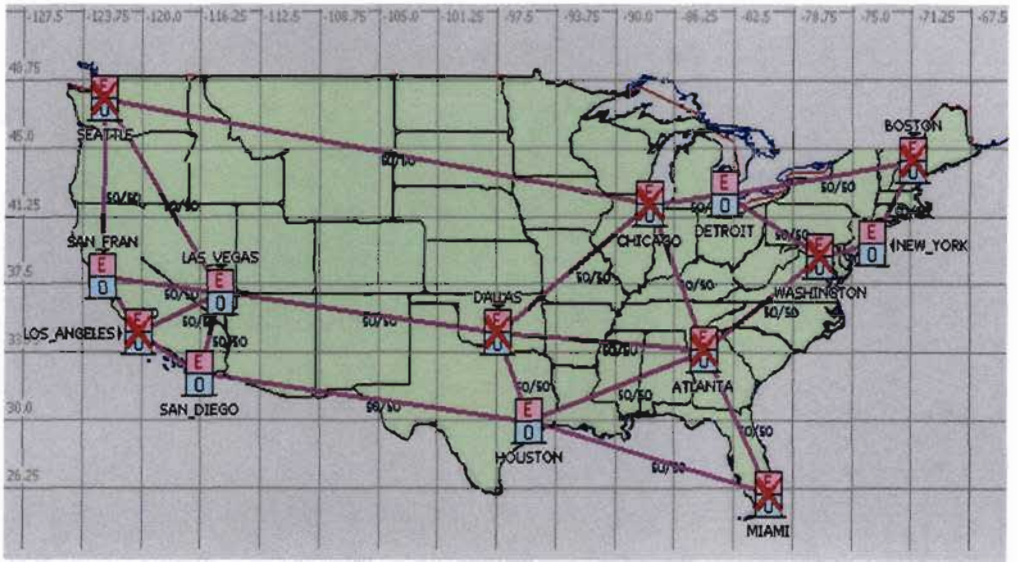


Figure C1-6 Model for 60% Node Failure

70% Node Failure

Nodes Failed 70%

1) Node SEATTLE (OTS)
2) Node DALLAS (OTS)
3) Node BOSTON (OTS)
4) Node LOS_ANGELES (OTS)
5) Node MIAMI (OTS)
6) Node CHICAGO (OTS)
7) Node WASHINGTON (OTS)
8) Node ATLANTA (OTS)
9) Node NEW_YORK (OTS)
10) Node LAS_VEGAS (OTS)

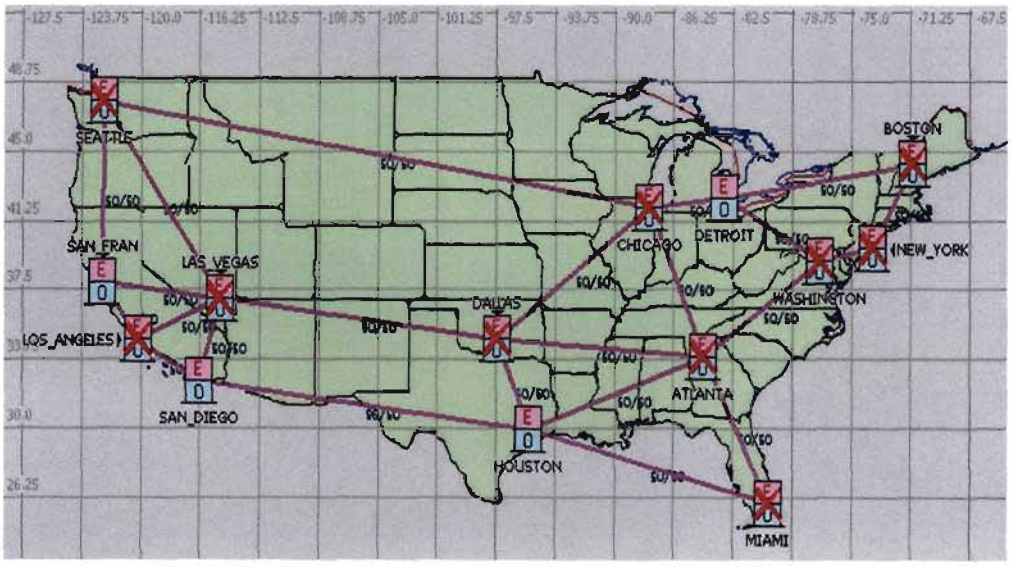


Figure C1-7 Model for 70% Node Failure

80% Node Failure

Nodes Failed 80%

1) Node SEATTLE (OTS)
2) Node DALLAS (OTS)
3) Node BOSTON (OTS)
4) Node LOS_ANGELES (OTS)
5) Node MIAMI (OTS)
6) Node CHICAGO (OTS)
7) Node WASHINGTON (OTS)
8) Node ATLANTA (OTS)
9) Node NEW_YORK (OTS)
10) Node LAS_VEGAS (OTS)
11) Node HOUSTON (OTS)

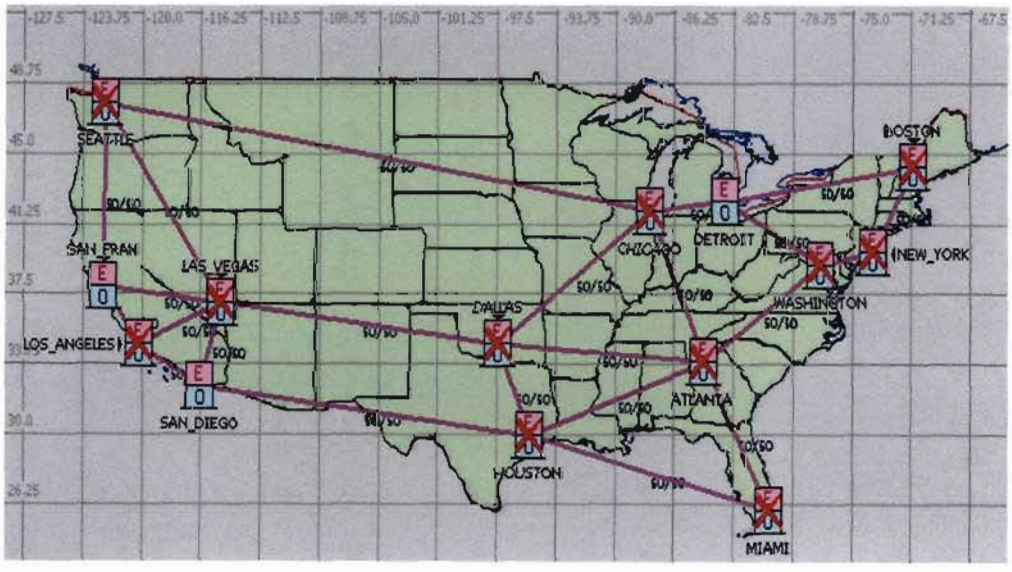
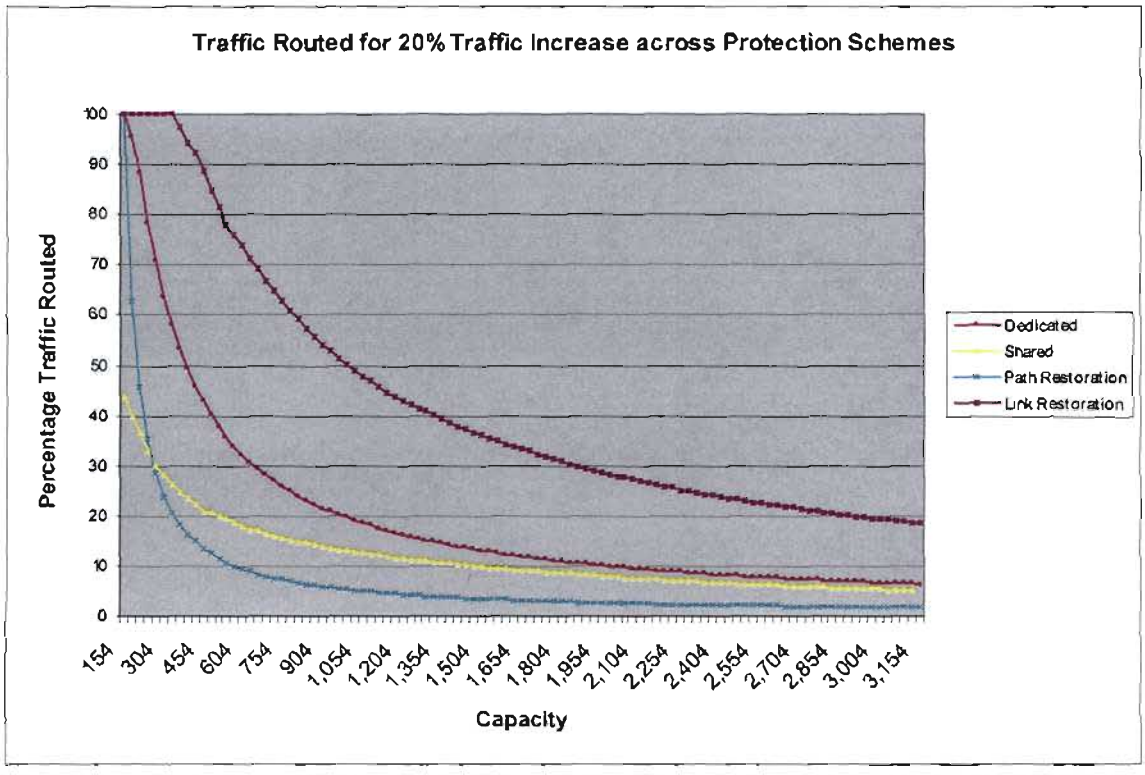


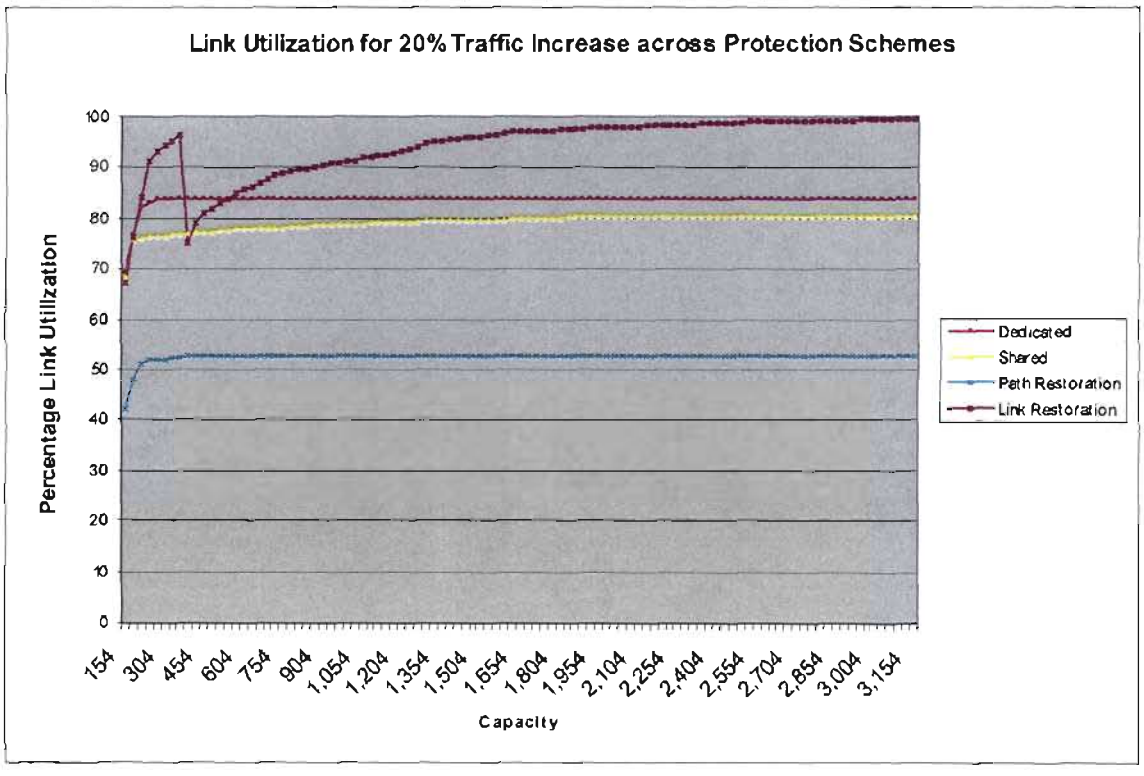
Figure C1-8 Model for 80% Node Failure

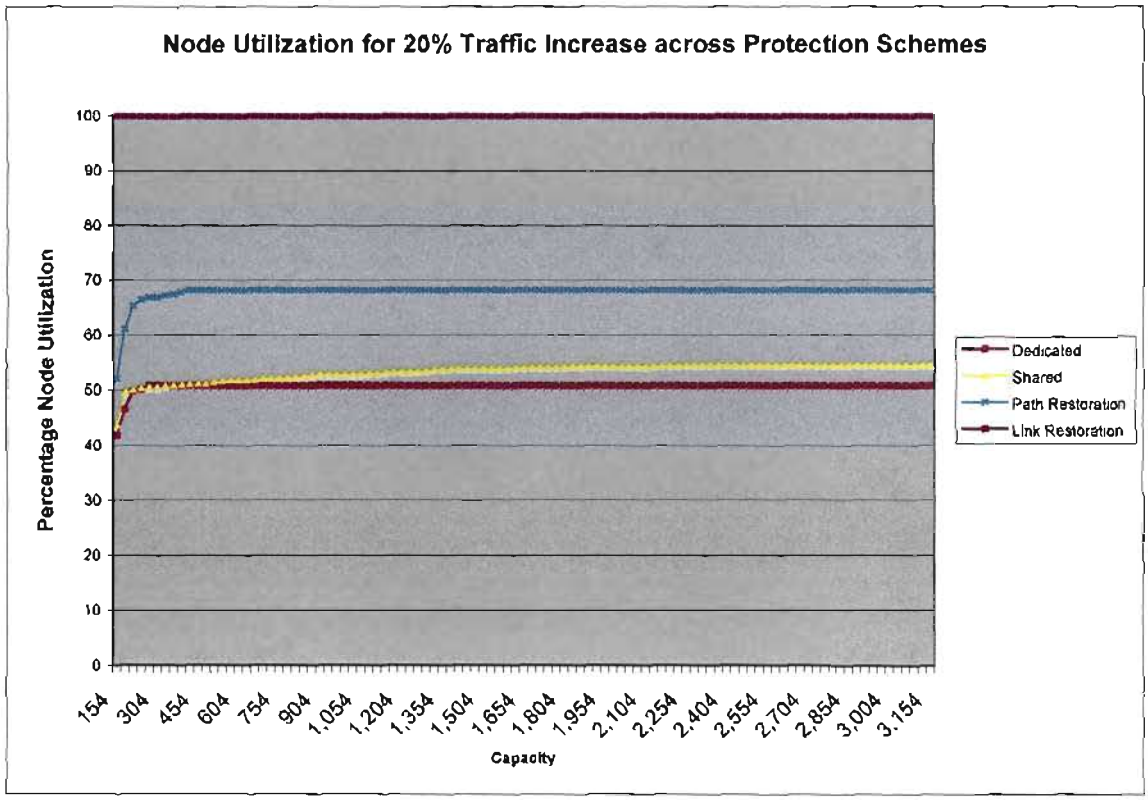
Appendix – D1

Plots of Numerical Data obtained for Traffic Variations

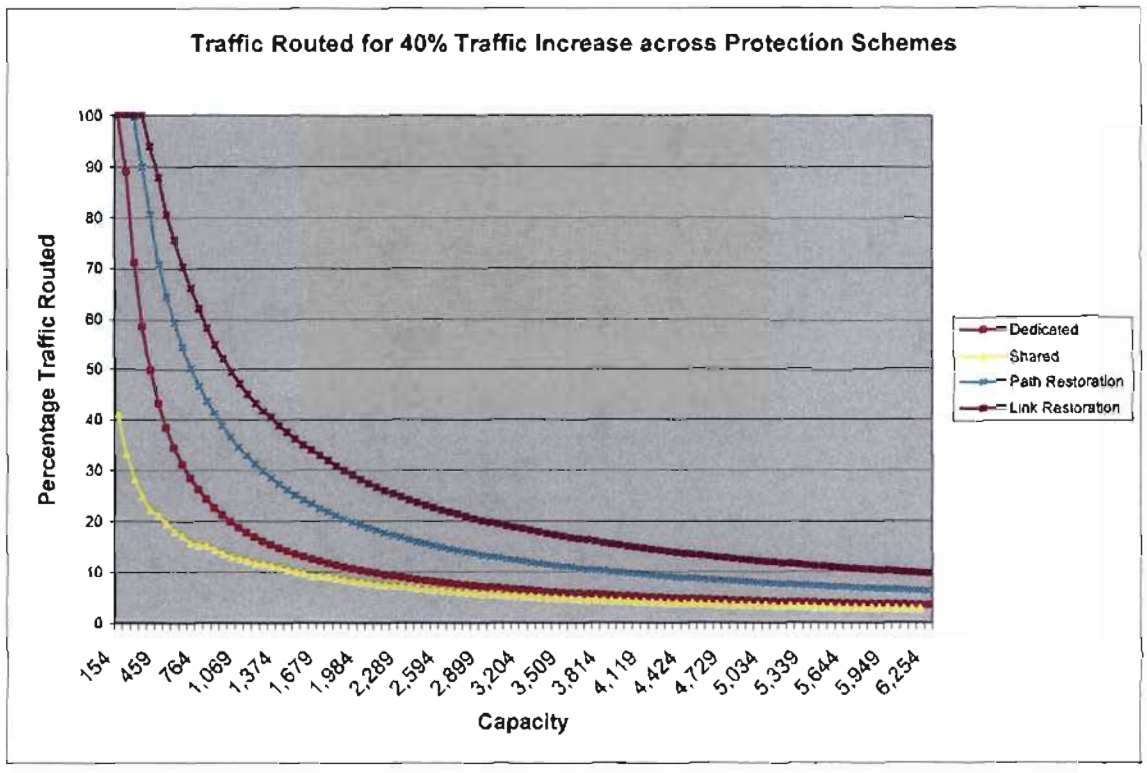
Plots for 20% Traffic Increase

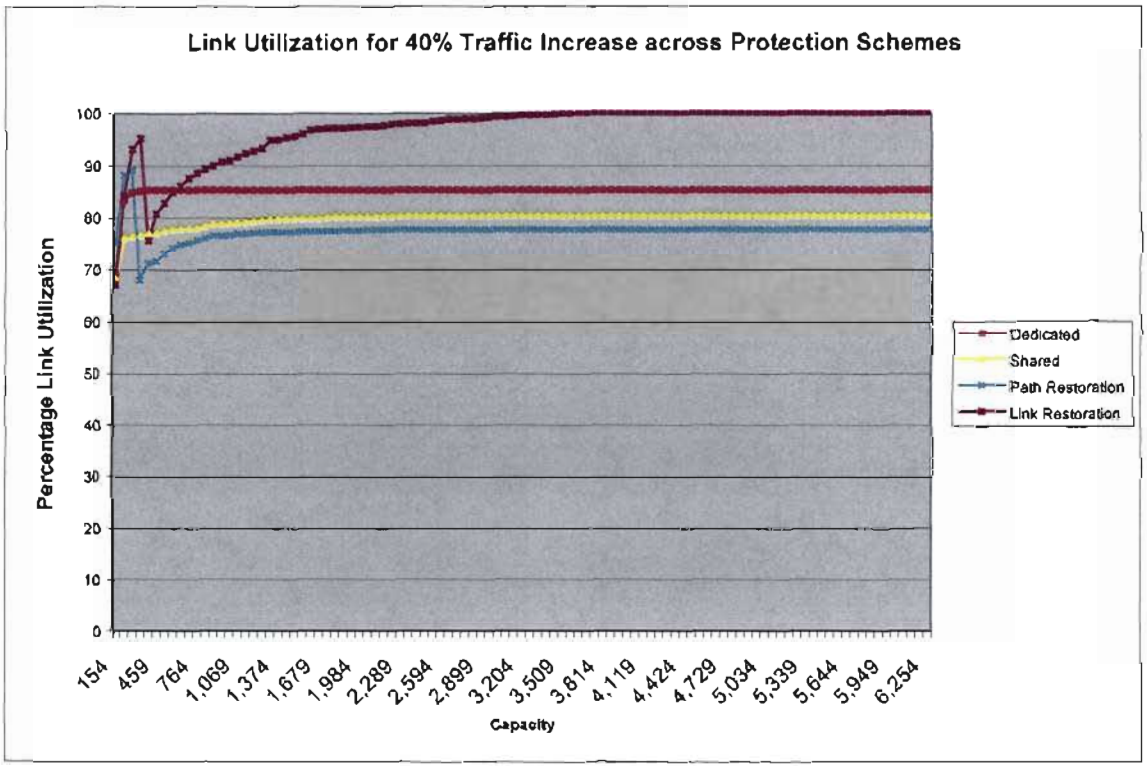


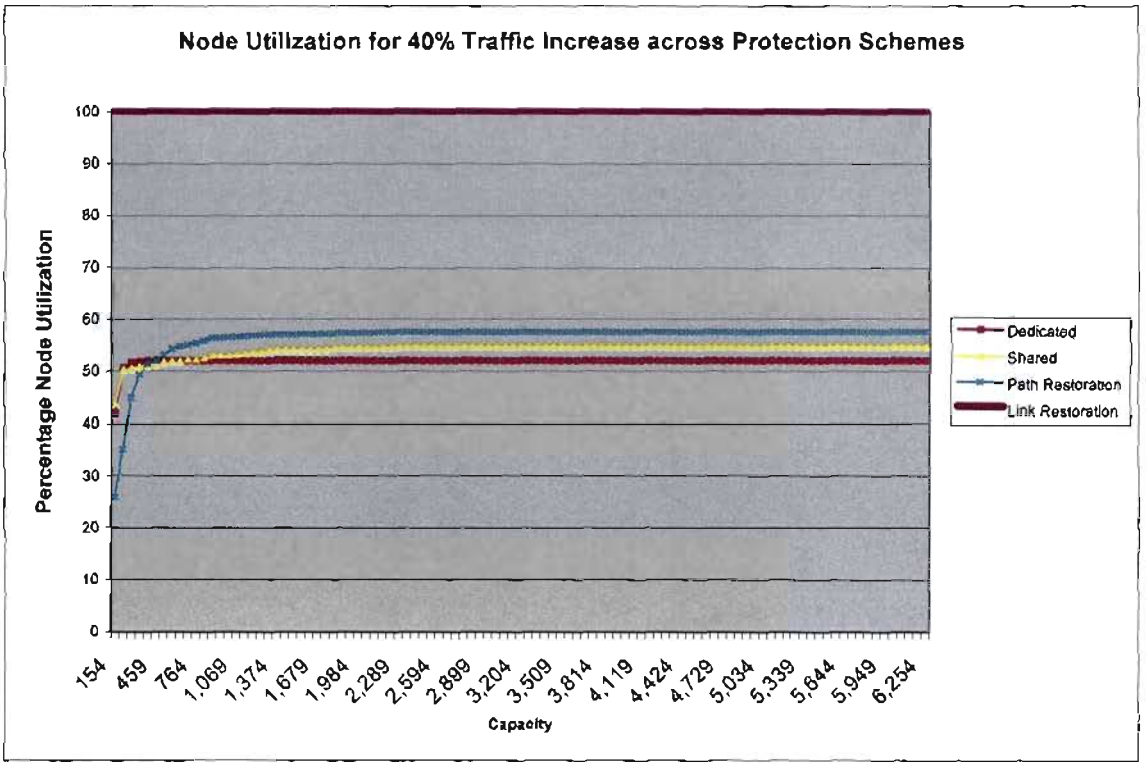



Node Utilization for 20% Traffic Increase across Protection Schemes
Percentage Node Utilization
100
90
80
70
60
50
40
30
20
10
0
154
304
454
604
754
904
1,054
1,204
1,354
1,504
1,654
1,804
1,954
2,104
2,254
2,404
2,554
2,704
2,854
3,004
3,154
Capacity
Dedicated
Shared
Path Restoration
Link Restoration

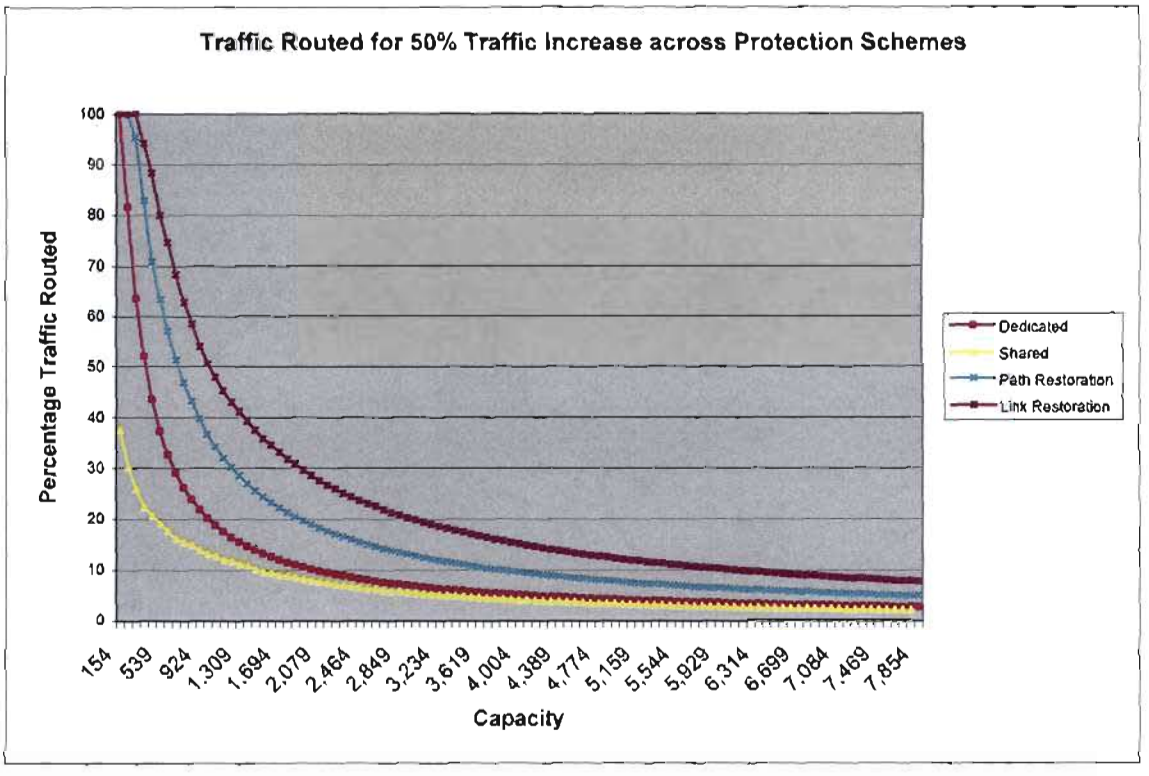
Plots for 40% Traffic Increase

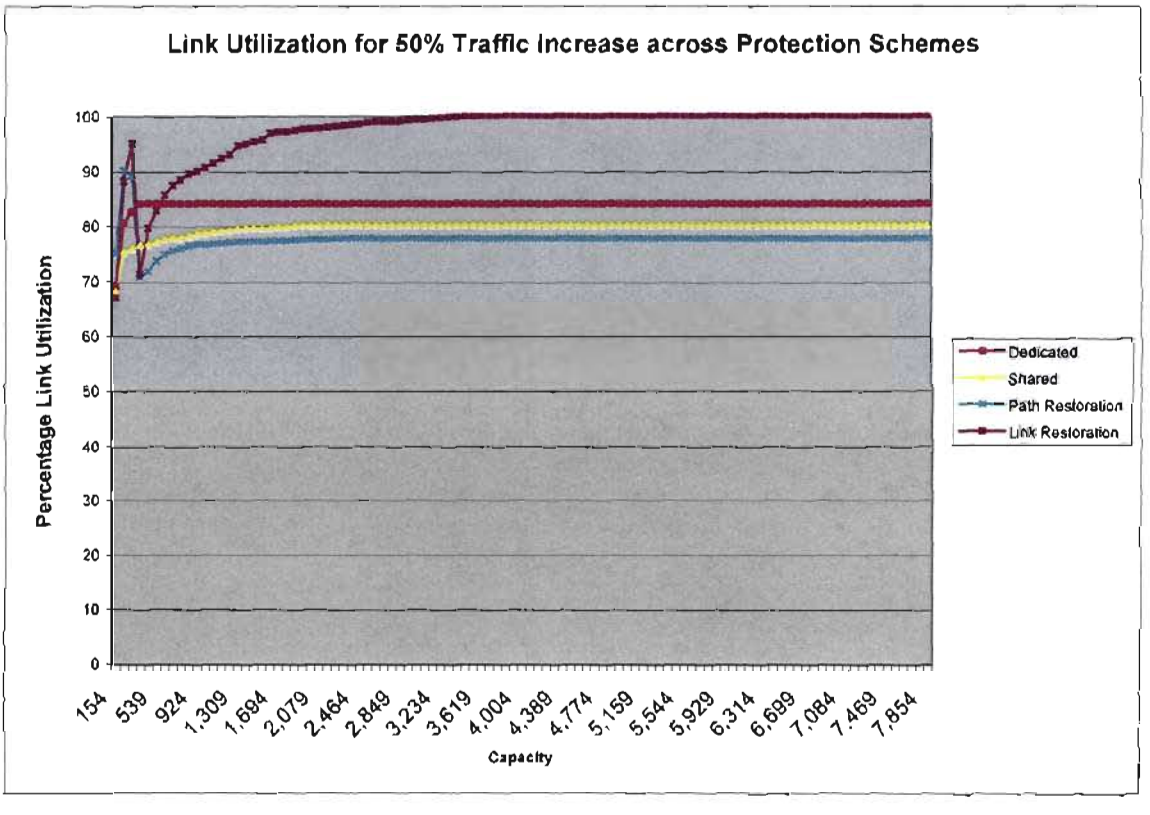


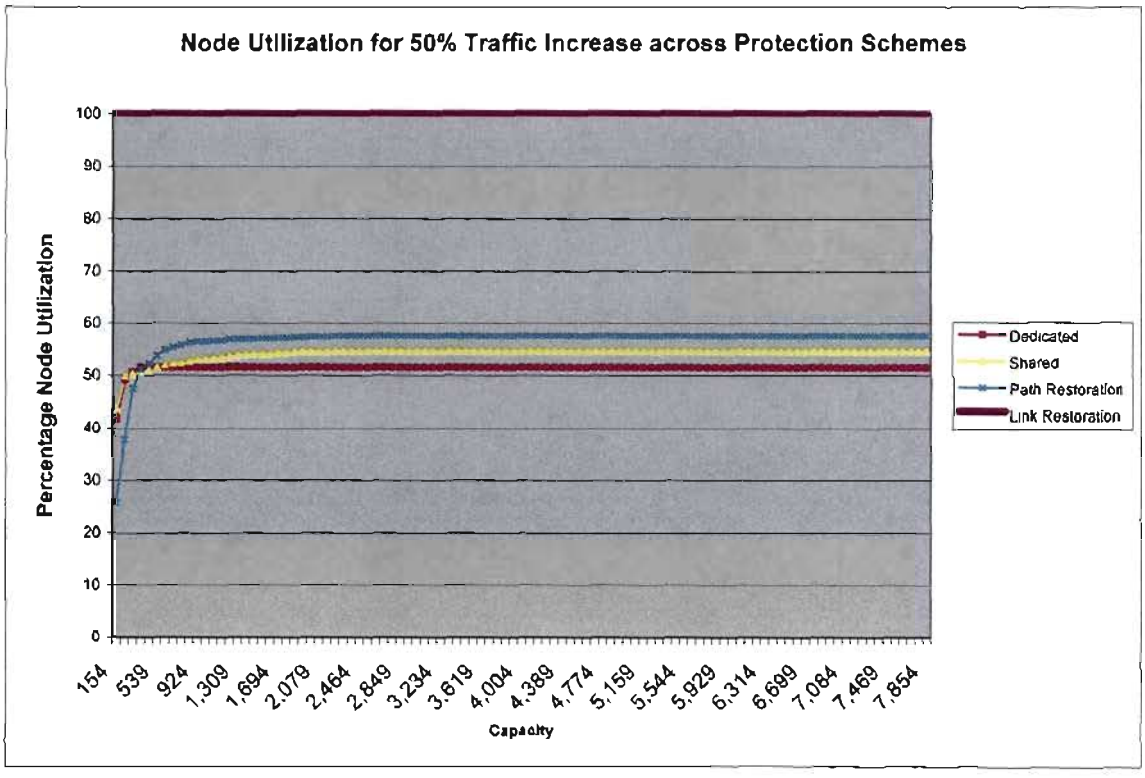



Node Utilization for 40% Traffic Increase across Protection Schemes
Percentage Node Utilization
100
90
80
70
60
50
40
30
20
10
0
154
459
764
1,069
1,374
1,679
1,984
2,289
2,594
2,899
3,204
3,509
3,814
4,119
4,424
4,729
5,034
5,339
5,644
5,949
6,254
Capacity
Dedicated
Shared
Path Restoration
Link Restoration

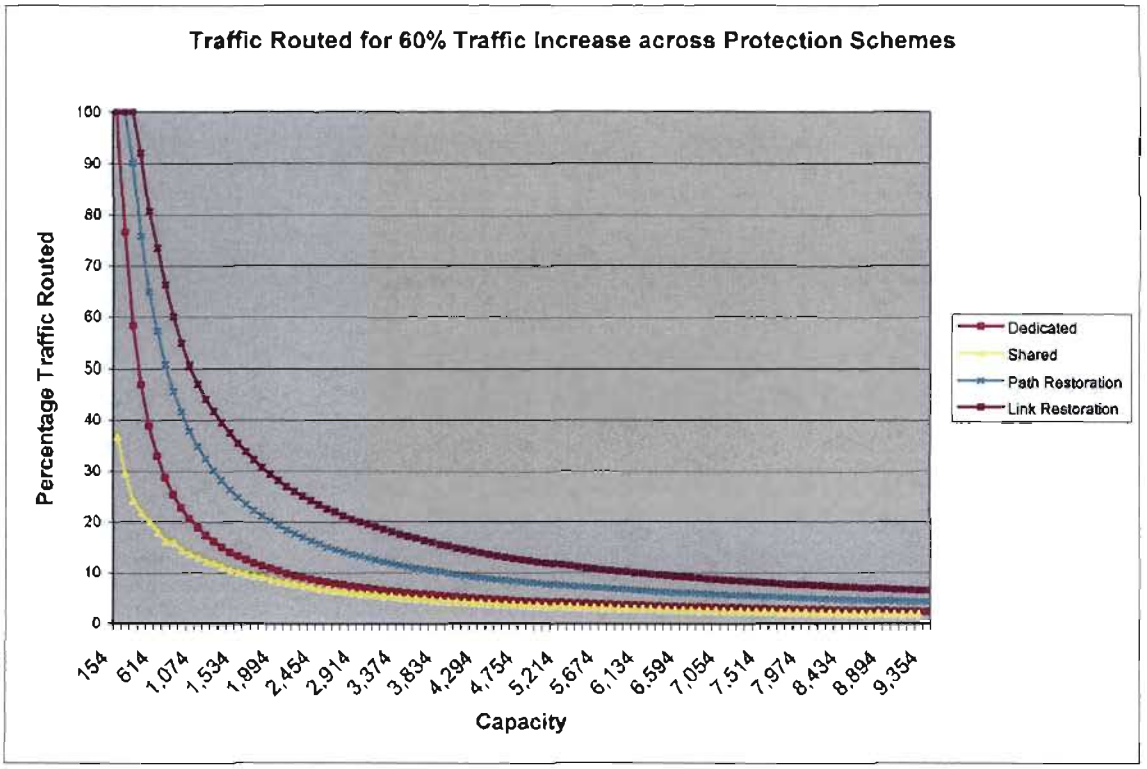
Plots for 50% Traffic Increase

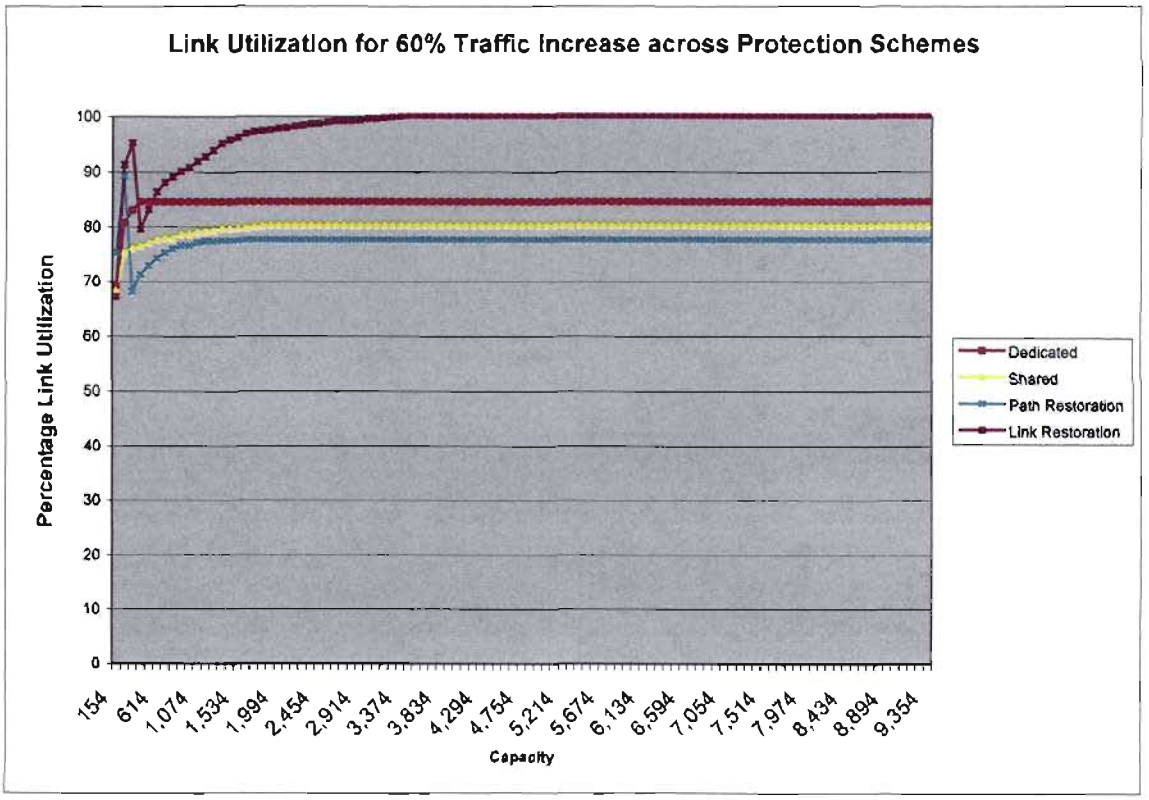


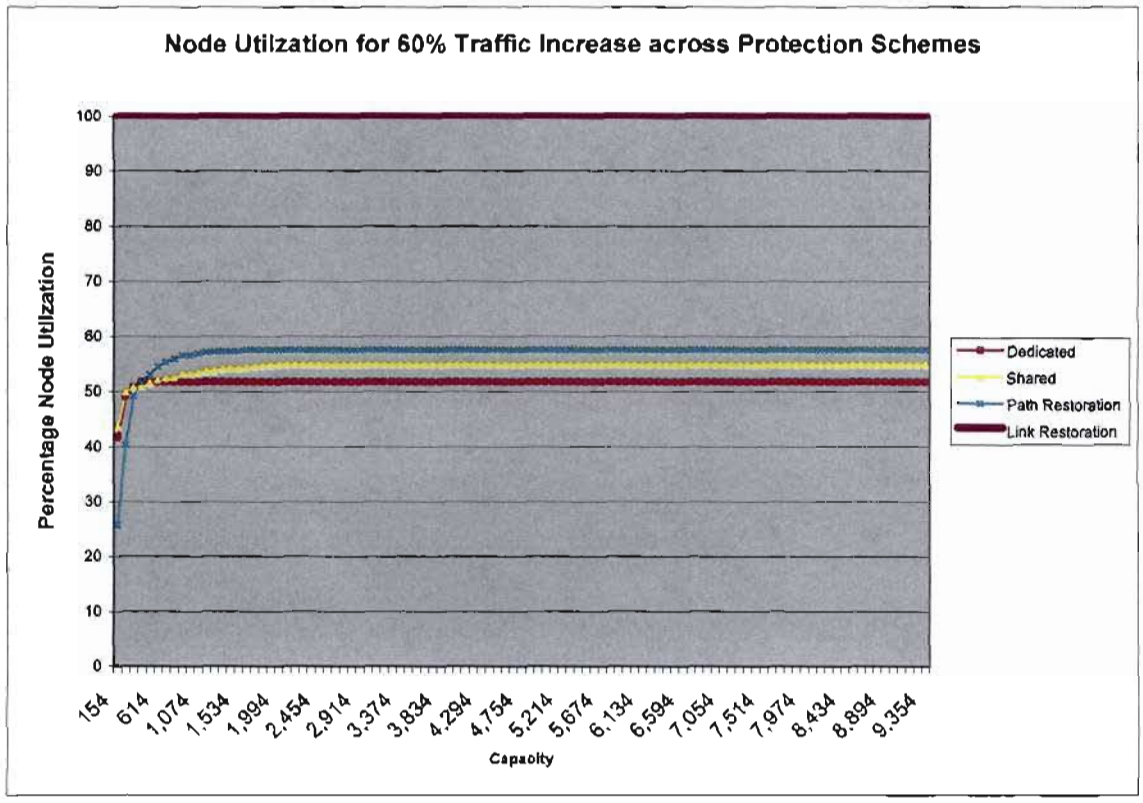



Node Utilization for 50% Traffic Increase across Protection Schemes
Percentage Node Utilization
100
90
80
70
60
50
40
30
20
10
0
154
539
924
1,309
1,694
2,079
2,464
2,849
3,234
3,619
4,004
4,389
4,774
5,159
5,544
5,929
6,314
6,699
7,084
7,469
7,854
Capacity
Dedicated
Shared
Path Restoration
Link Restoration

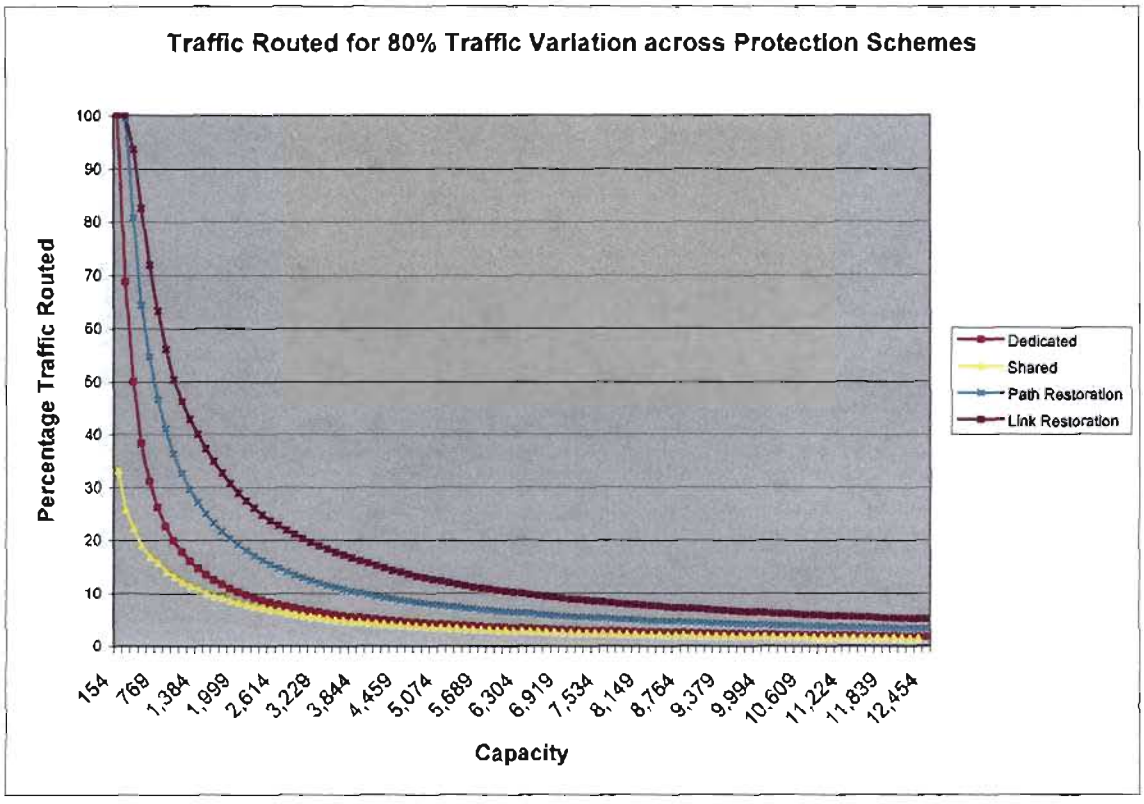
Plots for 60% Traffic Increase

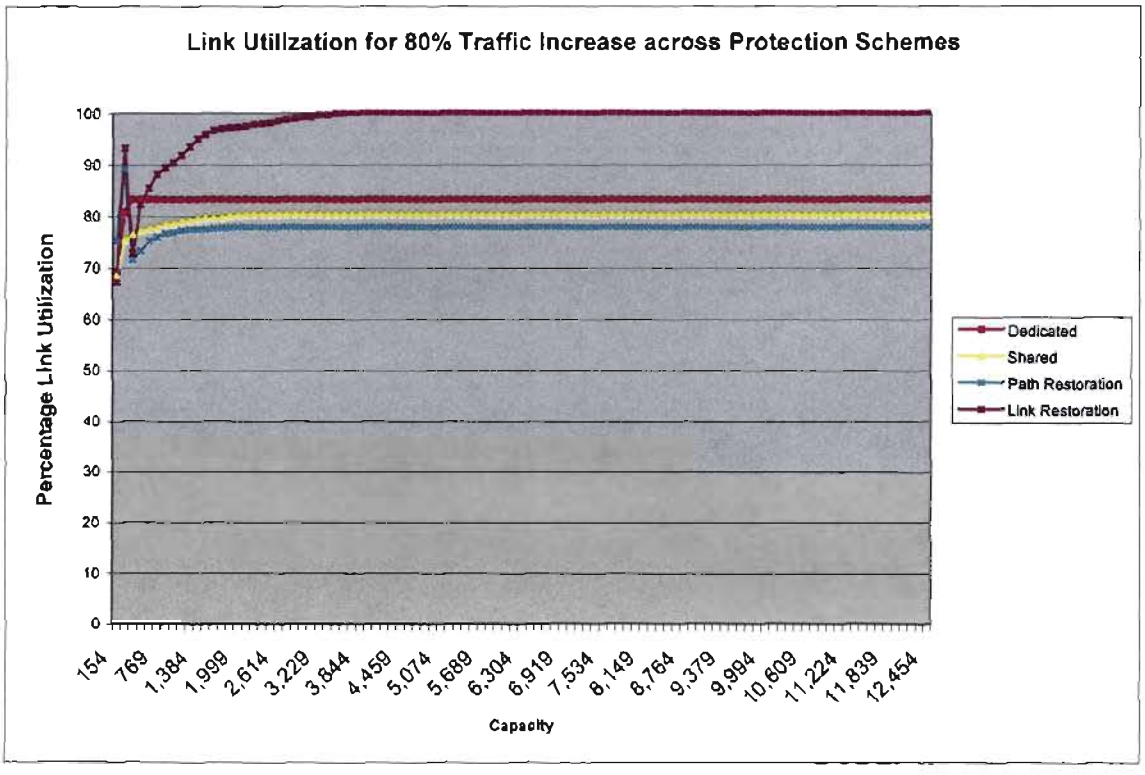


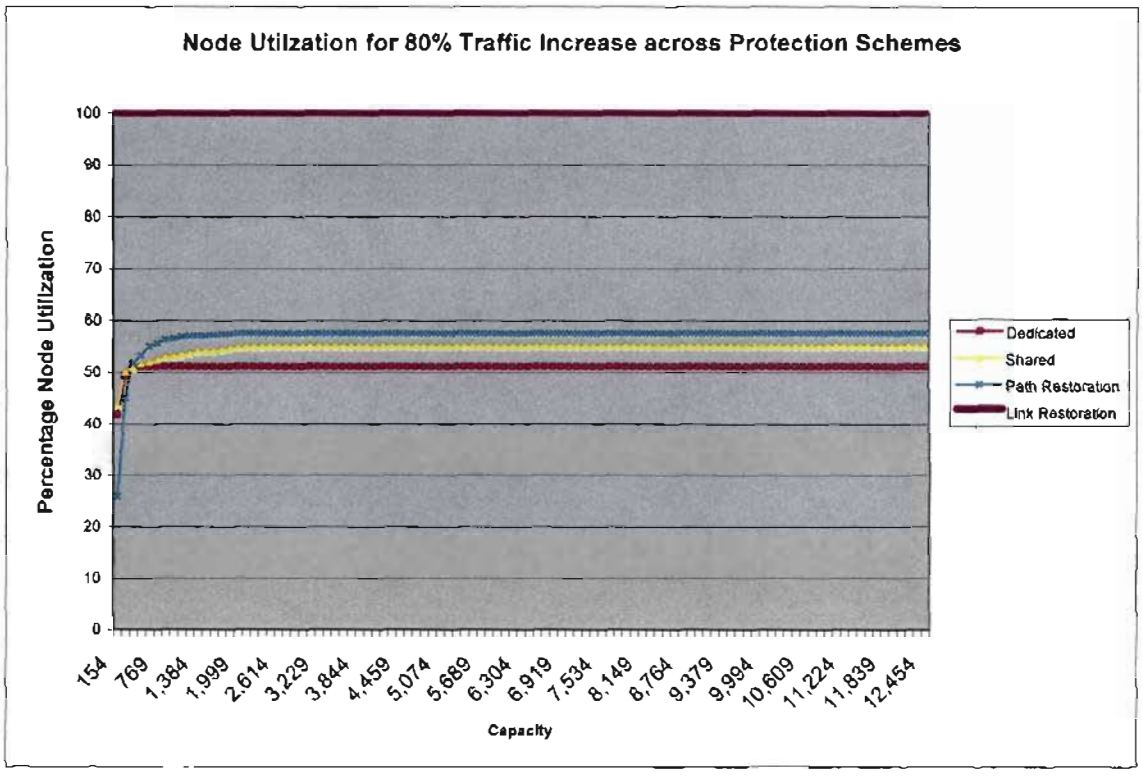



Node Utilization for 60% Traffic Increase across Protection Schemes
Percentage Node Utilization
100
90
80
70
60
50
40
30
20
10
0
154
614
1,074
1,534
1,994
2,454
2,914
3,374
3,834
4,294
4,754
5,214
5,674
6,134
6,594
7,054
7,514
7,974
8,434
8,894
9,354
Capacity
Dedicated
Shared
Path Restoration
Link Restoration

Plots for 80% Traffic Increase






Node Utilization for 80% Traffic Increase across Protection Schemes
Percentage Node Utilization
100
90
80
70
60
50
40
30
20
10
0
154
769
1,384
1,999
2,614
3,229
3,844
4,459
5,074
5,689
6,304
6,919
7,534
8,149
8,764
9,379
9,994
10,609
11,224
11,839
12,454
Capacity
Dedicated
Shared
Path Restoration
Link Restoration