PROVISIONING LIGHTPATH DEMANDS WITH QUALITY OF PROTECTION GRADES IN WDM OPTICAL NETWORKS

FENG ZHEMIN

NATIONAL UNIVERSITY OF SINGAPORE

2004

PROVISIONING LIGHTPATH DEMANDS WITH QUALITY OF PROTECTION GRADES IN WDM OPTICAL NETWORKS

FENG ZHEMIN

A THESIS SUBMITTED
FOR THE DEGREE OF MASTER OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
NATIONAL UNIVERSITY OF SINGAPORE

2004

Acknowledgements

I would express my deepest appreciation to my supervisor, Dr. Gurusamy Mohan. Dr. Mohan guided me through the work. His broad and in-depth knowledge, constant encouragement, and rigorous research style have great influence on me. I am always grateful to Dr. Mohan for his knowledge and his guidance.

I would like to acknowledge Dr. Chua Kee Chaing. Dr. Chua gave me a lot of help in my research work and gave me valuable suggestions in his busy time.

I am grateful to Ms. Tan Siok Kheng. Ms. Tan provided me resourceful information and patient help in my research work. I would also like to thank all my friends. They helped me a lot not only in my research study, but in my daily life in Singapore.

Thanks to National University of Singapore for grating me scholarship and the Open Source Software Laboratory for providing me the facilities.

Last but not least, with all my heart, I would like to thank my parents and my wife, for their understanding and consistent support.

Table of Contents

Summary

As the traffic in the Internet grows all day and all night, optical networks are emerging as the predominant transport layer technology for the next generation communication networks. Optical networking studies have been conducted over the past dozen years or so. This field has matured enormously over this time. Modern transport networks increasingly employ wavelength division multiplexing (WDM) technology to utilize the vast transmission bandwidth of fiber. WDM is based on transmission of data over separate wavelength channels on each fiber.

In a WDM optical network, the failure of network elements (e.g., fiber links and optical cross-connects) may cause the failure of several optical channels, therefore leading to large data loss. So the failure tolerance is an essential issue for a WDM network. A network with restoration capability requires redundant capacity to be used to give restoration guarantee, and a primary concern in designing such networks is to provide robustness with minimal redundancy.

Provisioning of a transport network refers to assigning network resources for a static traffic demand. Efficient provisioning is essential in minimizing the investment made on the network to accommodate a given demand. In WDM networks, provisioning means routing and wavelength selection for a set of end-to-end lightpath demands, given a demand distribution and a network topology, with the objective of minimizing the network resource usage.

In this thesis, Quality of Protection (QoP) is considered while provisioning survivable WDM networks. Different from the traditional protection schemes, QoP does not protect the entire traffic on the working path. Bandwidth is assigned to the backup paths according to the connection request's QoP grade, which in the range of 0 to 1, specifies the ratio of the backup bandwidth to the working bandwidth. Formulation of the problem is provided. Because the optimal solution to this problem is computationally intractable, heuristic solutions are developed for networks with and without wavelength continuity constraints. Simulations are conducted on two different network topologies and the results are discussed.

Key words: Wavelength division multiplexing, provisioning, survivability, quality of protection.

List of Figures

List of Tables

Chapter 1: Introduction

As networks face increasing bandwidth demand, network providers are moving towards a crucial milestone in network evolution: the optical network. Optical networks are high capacity telecommunication networks based on optical technologies and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength based services so that they provide higher capacity and reduced costs for new applications such as video and multimedia interaction, and advanced digital services.

1.1 History of Optical Networks

In the early 1980’s, a revolution in telecommunication networks began [1], spawned by the use of a new technology: fiber optic cable. From then on, the tremendous cost savings and increased network quality have led to a lot of improvement in the technologies for optical networks, the benefits of which began to be realized.

Telecommunication networks have evolved for almost a century time. Throughout this history, the digital network has evolved in three fundamental stages: asynchronous, synchronous, and optical networks. **Asynchronous Networks** were the first generation digital networks. In these networks, signals in each network element are transmitted according to its own internal clock. Besides the bit error issue caused by the difference of the clocks among the network components, it is hard for network providers to interconnect equipments from different vendors. The need for optical standards led to the emergence of the **synchronous optical network (SONET)** [2]. SONET specified the standards of line rates, coding schemes, bit-rate hierarchies, and operations and maintenance functionality. SONET also defined the types of network elements, network architectures that vendors could implement, and the functionality that each node in the network must perform. Since then, network providers could use different vendors' equipments, ensuring basic interoperability. As higher network speed is achieved, physical limitations in the laser sources and optical fiber begin to make the implementation of endlessly increasing the bit rate on each signal impractical. Customers are requiring more services and operations, and are carrying more and different types of data traffic. To provide full end-to-end connectivity, a new solution was needed to meet the high capacity and various needs. Wavelength Division Multiplexing (**WDM**) [3] optical networks provide enough bandwidth and flexibility to enable end-to-end wavelength services. WDM optical networks are based on wavelengths. This is the key difference between WDM optical network and other optical networks. The components of the WDM optical networks are defined according to how the wavelengths are transmitted, groomed, or implemented in the networks.

1.2 Benefits of WDM Optical Networks

Today, WDM is the best technology currently available to handle the rapidly increasing demand for bandwidth in telecommunications networks. In a WDM optical network, end users communicate with each other through all-optical channels called lightpaths. By wavelength multiplexing, these lightpaths offer huge bandwidth for users. In WDM optical networks, one can simply turn to a different color of light in the same fiber to achieve more bandwidth. Upgrading in WDM networks is much less expensive than the one that is necessary with a SONET/SDH solution. The most attracting feature of WDM is its low cost solution compared with its huge bandwidth capacity: three times cost will amount to 30 times the capacity [4]. Besides these benefits, WDM also provides a secure network, needs low power and requires low maintenance.

WDM itself provides the ability to establish lightpaths. This may greatly reduce the number of hops in the network. The fewer hops the traffic, the less queuing and intermediate processing are carried out in the network. This is very important to real time services. A lot of applications requiring **Quality of Service (QoS)** [5] [6] would benefit from having a single lightpath from one edge to the other edge of the network or from one major city to another major city just by having an optical cut-through (without optic-electric-optic conversion) lightpath. WDM also offers improved rerouting and protection switching and transparency in signals. It can carry a mix of analog and digital signals and protocols. Since it is protocol transparent, it does not matter what a wavelength is carrying in its payload. Although the initial deployments of WDM were point to point for transport, mesh topologies with more intelligence are now preferred by the users. Thus the WDM is evolving from a dumb tactical transport to an intelligent reconfigurable network layer technology.

1.3 Thesis Overview

1.3.1 Contribution

Similar to the concept of QoS, different classes of protection can be considered for optical networks [7]. According to the priority of the services in the network, different amount of network resources (lightpaths, ports, wavelength converters, etc.) are allocated to each connection to provide protection. Some of the connections in the network do not need full protection; they can even be preempted to provide necessary resources for more important connection. Based on this concept, how to minimize the network resource usage for a set of connections with different degrees of protection is an important issue in an IP/WDM network. It is well known that the optimal RWA problem is NP-complete for static lightpath establishment [8]. Since it is not practical to solve such problem for large-sized networks, heuristic algorithms are needed. We develop heuristic provisioning algorithms for a survivable WDM network with the concept of **Quality of Protection (QoP)** [9]. The QoP grade, in the range of 0 to 1, of a connection can be considered as the priority level of the connection in the network. The higher the QoP grade is, the more important the connection is. For each connection request, to protect the primary path in the event of failure, reduced bandwidth is allocated to the backup path if the QoP grade is less than 1. Suppose that the bandwidth on the primary path for a connection request is 1 unit in terms of wavelength capacity, and the QoP grade of this connection request is 0.3. The bandwidth on the backup path for this connection request is $1\times 0.3 = 0.3$ units, not 1 as in traditional full protection schemes. So, for each connection request, the bandwidth reserved for backup path is significantly reduced. Connections traversing the same primary physical path also share the same risk of failure such that these connections can use the same backup path. Hence the bandwidth is efficiently utilized. Load balancing (i.e., uniform wavelength usage) is a desired feature in routing policy for WDM networks, and it consists in distributing the load as much as possible on the network in order to delay the occurrence of congestion. Hence, future requests will be accepted with higher probability in a load balanced network than in a load un-balanced network. To achieve load balancing after provisioning the connection request, we check the maximum number of wavelengths in the network. If the load in the network is un-balanced, rerouting and re-assigning wavelengths for some of the connection requests is necessary. First, we study the case for WDM networks with wavelength convertibility. This algorithm can also be modified to apply to WDM networks without wavelength convertibility. Simulation was carried out to test the performance of this algorithm on networks with different topologies. In networks with unlimited number of wavelengths, the objective is to minimize the total number of wavelengths used. While in networks with limited number of wavelengths, the objective is to maximize the total number of acceptable connection requests. The performance of our algorithm is also studied in networks with/without wavelength limit. We compare the performance of our algorithm with that of the full protection schemes. We discuss the results, explaining the factors that affect the performance of our algorithm.

1.3.2 Thesis Organization

The thesis is organized into five chapters. The content of each chapter is summarized as given bellow:

Chapter2 presents protection and provisioning issues in WDM networks. Related work in these areas is presented. Formulation of the provisioning problem in survivable WDM networks with QoP concept is presented. *Chapter3* provides heuristic solutions to the provisioning problem, including multi-path searching, wavelength assignment and load balancing. Simulation results and analysis are also presented in this chapter. *Chapter4* presents a provisioning method proposed and simulation results in a network with wavelength continuity constraints. *Chapter5* makes concluding remarks and discusses the future work.

Chapter 2: Basic Concepts and Problem Definition

In the future, **IP-over-WDM** (also referred to as IP/WDM) [4] layering will depend on the ability of the IP layer to provide quality of service. Also, it would depend on whether the WDM network would be survivable and as robust as the SONET/SDH. The rate of evolution would also depend on whether the interfaces would be cheap enough for the IP-over-WDM to be commercially attractive.

2.1 Architecture of IP-over-WDM Networks

The development of IP/WDM technology and networking architecture can be classified into three generations [10]: (i) **IP over Point-to-Point DWDM**, (ii) **IP over Reconfigurable WDM**, (iii) **IP over Switched WDM**.

2.1.1 IP over Point-to-Point DWDM

Dense WDM (DWDM) [11] systems are deployed in the first generation for point-to-point high-bandwidth communication among routers. Usually, SONET takes charge of framing and transporting overhead information on the WDM channels. SONET encapsulates IP packets in its frames with Packet-over-SONET schemes for later transportation.. Figure 2.1 shows the architecture of IP over point-to-point WDM network.

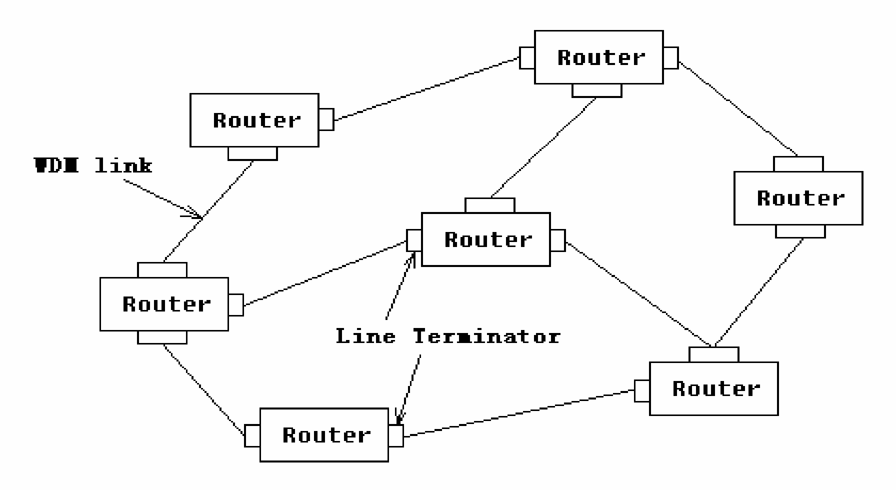


Figure 2.1 Architecture of an IP over point-to-point WDM network

In an IP over point-to-point DWDM architecture, IP routers directly connect with their peers through multi-wavelength fiber links. In this architecture, the network topology is fixed, and the network configurations are all static. Management systems for such networks are usually centralized, and the interaction between the IP layer and WDM layer is least compared with other architectures.

2.1.2 IP over Reconfigurable WDM

The second generation IP/WDM system is IP over reconfigurable WDM network. In this architecture, WDM channels are routed in the WDM network with WDM cross-connects. It utilizes the WDM bandwidth more efficiently than the first generation networks. Due to the ability of reconfiguration implemented in this generation of products, it is possible to move protection switching and restoration directly into the optical layer, thereby eliminating the need for the SONET layer between the IP layer and the optical layer. **Wavelength cross-connect (WXC)** [3] is the key component in this network architecture. A WXC can switch the traffic from any of its input port to any of its output port. Figure 2.2 illustrates how the components are connected with each other. In this architecture, the WXCs are interconnected in a mesh configuration with multi-wavelength WDM fiber links as service layer and the IP layer as the client layer. By appropriately configuring the WXCs, a given router interface can be connected to any other one at any other router. Therefore, such configuration provides a flexible interface for the routers.

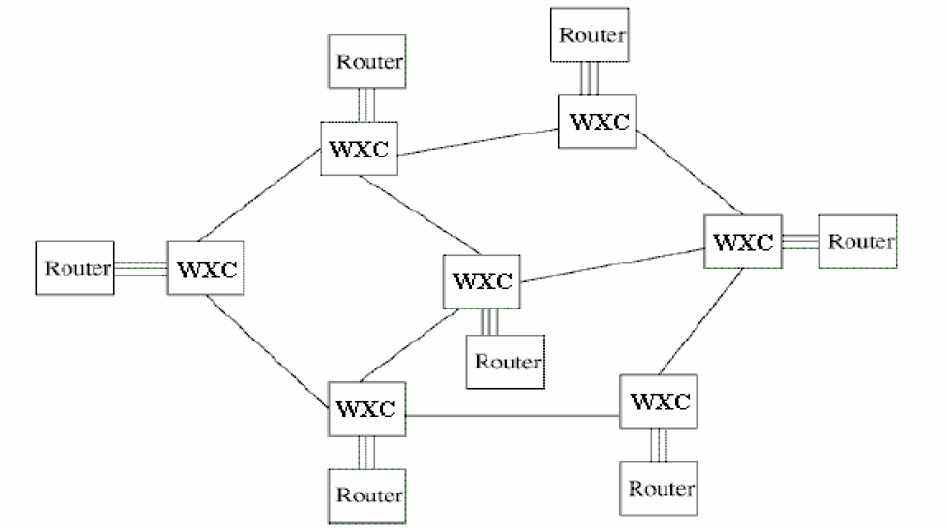


Figure 2.2 Architecture of an IP over reconfigurable WDM network [10]

Due to the flexibility of this architecture, several different models:

- **Overlay model.** The IP layer and WDM layer interact like a client-server mode, with IP being the client layer and WDM layer being the server layer. The routers in IP network layer connect with their neighbours through the

Wavelength Add/Drop Multiplexer (**WADM**) [3] and WXC (or **OXC**, Optical Cross-Connect) in the WDM layer. Both the layers provide the management and control functions for themselves, and well-defined interfaces provide the interaction between the two layers.

- **Integrated model.** The IP layer and WDM layer are merged into one single layer. In this model, the IP router and the OXC are integrated together and exist as a single network element. **Multi-Protocol Label Switching (MPLS)** [12] [13] and its lambda variant (MPλS) are used to provide the management and control plane in this model.
- **Peering model.** Devices in each of the two layers interact in a peer-to-peer relationship. In this model, MPLS and its lambda variant MPλS still provide the management and control plane. However, unlike the integrated model, where the IP routers and OXCs employ a common addressing plan, exterior gateway protocols provide the two layers different routing and signaling domains such that the routers and the OXCs interact with each other like peers in the network just like in a single layer.

2.1.3 IP over Switched WDM

In the third generation of IP/WDM systems, i.e. IP over Switched WDM networks, WDM packet switches directly transport the IP packets. In laboratory trials, WDM packet-switches have been demonstrated successfully, including in the DARPA funded **Optical Label Switching Project** [14]. In this architecture, the WDM layer directly supports per-packet-switching capability, as opposed to simply providing ingress-to-egress lightpaths. Hence, a much finer grain sharing than IP over point-to-point and re-configurable WDM can be provided in this structure. Several WDM switching approaches have been proposed, including **Optical Burst Switching (OBS)** [15] [16] [17], and **Optical Label Switching (OLS)** [14].

2.2 Issues in WDM Optical Networks

As IP/WDM networking architecture matures from a point-to-point architecture towards more dynamic re-configurable and switched architecture, two main trends come with the increasing flexibility and agility in networking equipments:

- A shift-away from static planned resource allocation and service provisioning, towards dynamic on-demand resource allocation and service provisioning.
- A shift-away from centralized management and off-line optimization strategies towards distributed control and on-line heuristics in network and traffic management.

In recent years, as telecommunication networks face explosive IP traffic growth, management and control system in the IP/WDM networks have to become more intelligent to produce a more autonomous network, thereby simplifying and reducing the cost of network operations [17] [18] [19]. In this condition, several management and control issues are worth of studying.

2.2.1 IP/WDM Configuration and Routing

Reconfigurable IP/WDM networks raise new issues concerning the routing in optical networks. Optical layer control planes based on MPLS and other Internet protocols hold great promise because of their proven scalability, ability to support rapid provisioning, and auto discovery and self-inventory capabilities [20]. Wavelength circuit routing may be carried out by link state routing protocols. However, it is not the same as IP layer routing because WDM layer routing must be load dependent. That means that a WDM fiber cannot admit new wavelength circuit when all its wavelength channels are consumed.

Another routing issue in IP over reconfigurable WDM networks is that wavelength routing is affected if the OXCs in the network can perform wavelength conversion. Wavelength conversion helps to reduce connection blocking probabilities. Optical wavelength-conversion technology is very expensive at present. Hence all-optical cross-connects that support wavelength conversion have to be deployed sparingly in the network. Depending on the capability of the cross-connects, the wavelength routing algorithm has to consider the wavelength continuity constraint.

2.2.2 IP/WDM Fault Localization and Recovery

To utilize IP/WDM networks' tremendous traffic capacity in the next generation Internet, the network must provide fault management techniques to combat fiber failures which will cause huge data loss if no protection is provided [21].

Fault detection and localization in IP/WDM networks was more difficult compared with the fault localization only in IP layer. The problem becomes even more complex in IP over re-configurable WDM networks, because the wavelength circuits in the WDM layer may change from time to time. The parameters provided by the optical WDM layer are mostly low level analog signal parameters such as optical signal power, optical SNR, and wavelength registration measurements [22] bearing no fixed definitive relations to the high level IP layer observable properties. Because WDM monitors analog signal parameters, to determine if failure occurs, the WDM layer has to detect a crossing of threshold values. Setting a combination of such different threshold values makes the fault localization complicated. Another complexity arises from different signal processing and fault propagation characteristics in different WDM equipments. Because of these complexities, effective IP/WDM fault detection and localization requires high integration across both IP and WDM. An integrated fault model that encompasses hard and soft metrics from both IP and WDM layers is necessary. This is an area that requires much additional research.

The main objective of network fault recovery is to keep the upper layer, i.e. IP layer, working even when part of the network elements cannot work as normal. In IP-over-WDM networks, network survivability is provided by protection and restoration facility in the SONET layer. This can be achieved in several different ways:

- **Server approach**: In overlay model, IP layer and WDM layer are totally separate, and the WDM layer works as a server to provide wavelength circuits for the client layer: IP layer. In this case, the large amount of data can be recovered by protecting the wavelength circuits in the server layer.
- **Client approach**: The IP layer itself has the capability to employ distributed routing algorithm which deals with the change of the network topology in the event of failures. Such algorithm can also provide dynamic routing to achieve network recovery as in the WDM layer.
- **Integrated approach**: As the MPLS technology matures, an integrated control plane can be used such that the recovery can be approached through MPLS/$MP\lambda S$ [23] [24]. In MPLS networks, traffic is transported through **Label Switched Paths** (**LSP**s) [25]. When failure occurs, primary LSP affected by the failure can be quickly switched to the backup LSP. The main advantage of this scheme is that MPLS provides the coordination between the IP components and WDM components.

2.2.3 IP/WDM Traffic Engineering and Load Balancing

The flexibility in dynamic IP/WDM networks not only provides dynamic network configuration, but also provides the capability to perform traffic engineering such that the network performance can be optimized and network resource can be efficiently utilized.

Traditional IP networks employ destination-based **Shortest Path First (SPF)** routing to forward traffic from source to destination. This algorithm is simple and stable, and works well when the network is lightly loaded. However, the drawback is that it does not consider the traffic load in the network and does not support diverse routes. The first scheme proposed for load balancing in IP networks is **ECMP** (Equal Cost Multi-Paths) which was described by Moy [26]. ECMP states that all equal cost paths between the source and destination can be used such that the traffic between the two ends can be divided into several parts to be evenly distributed the traffic in the networks. However, the ECMP routing is traffic independent in the sense that there is no load balancing between the multiple paths, because there is also no feedback between the traffic load and the routing algorithm. A further enhancement to ECMP for load balancing, called Optimized Multi-Path Routing (**OMP**), has been proposed in [27]. OMP utilizes a link-state routing protocol to broadcast link loading information periodically. The routing algorithm utilizes the link-loading information to split the traffic load among multiple near-equal cost paths.

As MPLS emerged to support IP traffic engineering needs, the routing and forwarding functions in IP layer are separated. MPLS supports constraint based routing, including in particular explicit routing, thereby allowing direct control on the exact paths of IP traffic. In an IP over re-configurable WDM network, traffic engineering can also be affected through wavelength circuit reconfiguration that adapts the IP network (virtual) topology to the evolving traffic pattern.

2.3 Network Survivability

Providing resilience against failure is an important requirement for many high-speed networks. A single fiber failure can disrupt millions of users and result in millions of dollars of lost revenue to users and operators of networks. In optical layer, many protection schemes have been designed to provide network survivability in mesh topology.

2.3.1 Basic Protection Concepts

Recovery schemes can be classified into two categories: **Protection Schemes**, and **Restoration Schemes** [28]. In protection schemes, pre-allocated backup path can be used immediately when failure occurs along the primary path. While in restoration schemes, no pre-allocated backup path is reserved at any time. The backup resources are allocated and utilized only when failure occurs. So the restoration schemes are dynamic. Protection schemes are simpler and faster then the restoration schemes. However, this is achieved with the expense of more network resource allocation. In protection schemes, network resources are not utilized as efficiently as in restoration schemes.

Protection maybe **dedicated** or **shared** [3]. In dedicated protection, each working path is assigned its own dedicated backup path in the network over which it can be rerouted in case of a failure. In shared protection, we make use of the fact that not all working connections in the network fail simultaneously (for example, if they are in different parts of the network). Therefore, we can make multiple working connections share protection bandwidth only if no more than one of them fails at any specific time. This helps to reduce the bandwidth needed in the network to provide survivability. Another advantage of shared protection is that the protection bandwidth can be used to carry low-priority traffic when no failure occurs in the network. This low-priority traffic is discarded in the event of a failure when the bandwidth is needed to protect a connection. Figure 2.3 shows the difference of these two schemes.

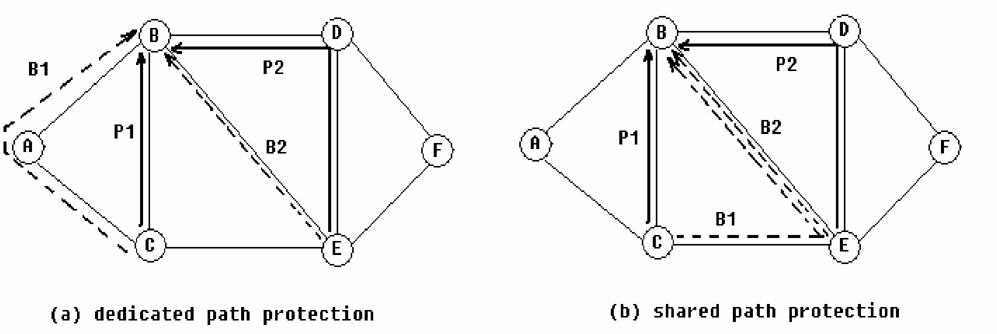


Figure 2.3 Dedicated Path Protection & Shared Path Protection [3]

In Figure 2.3.a, two primary paths (P1 and P2) have link disjoint backup paths (B1 and B2). So we say that P1 and P2 are exclusively protected. While in Figure 2.3.b, the two backup paths share a common link (E, B), i.e., link (E, B) provides protection for both P1 and P2. In this case, wavelength used for backup paths is shared. When single-link failure model is assumed, it does not pose any problem since P1 and P2 are link-disjoint.

2.3.2 Optical Layer Protection Schemes

The optical layer provides lightpaths for use by its client layers, such as SONET, IP, or ATM layers. Optical protection schemes also belong to the optical channel (OCh) layer or optical multiplex section (OMS) layers [28]. An OCh layer scheme restores one lightpath at a time, whereas an OMS layer scheme restores the entire group of lightpaths on a link and cannot restore individual lightpaths separately. Table 2.1 [28] provides an overview of the schemes operating in the optical multiplex section layer. Table 2.2 [28] summarizes schemes operating in the optical channel layer.

Table 2.1 Protection Schemes Operating in OMS Layer

	Protection Schemes			
	1+1	**1:1**	**OMS-DPRing**	**OMS-SPRing**
Type	Dedicated	Shared	Dedicated	Shared
Topology	Point-to-point	Point-to-point	Ring	Ring

Table 2.2 Protection Schemes Operating in OCh Layer

	Protection Schemes		
	1+1	**OCh-SPRing**	**OCh-Mesh**
Type	Dedicated	Shared	Shared
Topology	Mesh	Ring	Mesh

There can be a significant difference in cost associated with OCh layer schemes relative to OMS layer schemes. An OCh layer scheme has to demultiplex all the wavelengths, whereas an OMS layer scheme operates on all the wavelengths and thus requires less equipment. Figure 2.4 shows the difference of the two schemes [28].

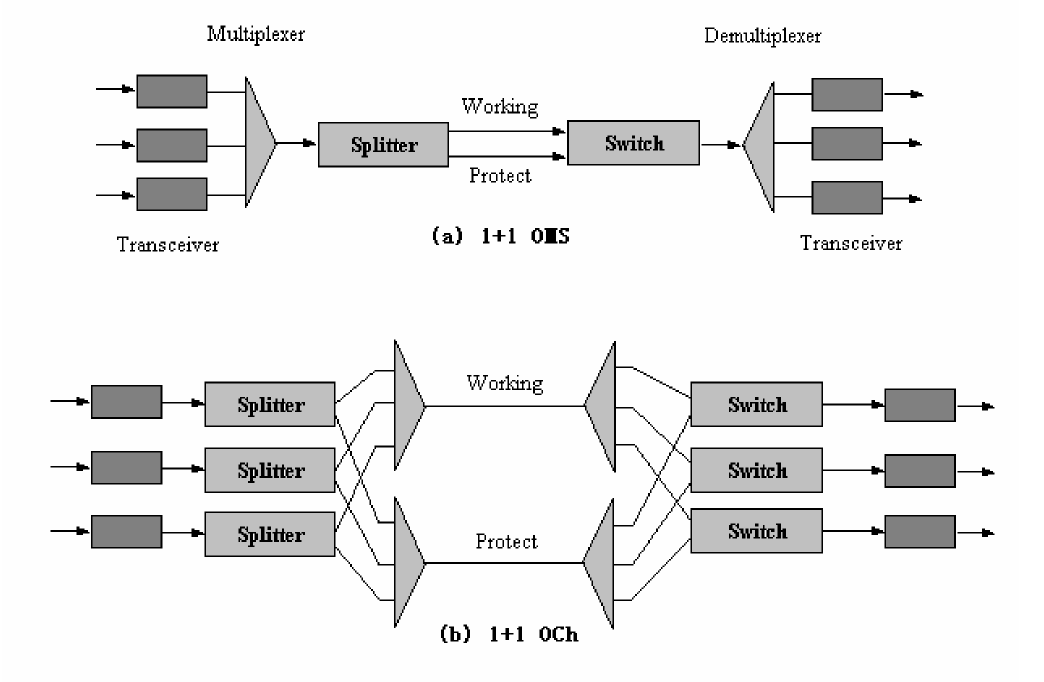


Figure 2.4 Comparison of (a) 1+1 OMS and (b) 1+1 OCh

The most commonly deployed protection architectures are **1+1** and **1:1** [28]. In **1+1** architecture, data are transmitted in both primary and secondary paths, where the destination picks up the better-quality signal. The **1+1** architecture scheme does not support extra traffic since the primary and the secondary paths carry the same traffic simultaneously. To prevent data loss, the source node should delay transmitting data on the secondary path for a certain amount of time, depending on the difference in the propagation delays between primary and secondary paths, plus the fault detection time. There are two types of **1:1** protection. In one type, a dedicated protection path is required, but the protection path is allocated to carry low-priority traffic under normal circumstances. In the second case, the protection path is not dedicated and multiple protection lightpaths can share the same resources in the protection path as long as there is no shared link among their associated working lightpaths. The **1:1** protection scheme can be extended to **M:N** protection, which uses N protection lightpaths to protect the traffic on M working lightpaths. Apparently, **1+1** architecture is faster and simpler than **1:1** architecture but at the expense of lower network utilization

2.4 Provisioning and Load Balancing

Provisioning of a transport network refers to assigning network resources to a set of static traffic demand [29]. Efficient provisioning is essential in minimizing the investment made on the network required to accommodate a given demand. Naturally, provisioning of WDM networks has been the subject of considerable interest. This interest concentrates on roughly two categories of settings: the case of limited deployed fiber, where provisioning seeks to minimize the number of required wavelengths, and the case of limited number of wavelengths per fiber, where provisioning seeks to minimize the amount of required fiber, or to maximize the accommodated traffic.

2.4.1 Routing and Wavelength Assignments (RWA)

Given a set of connection requests, the problem of setting up of lightpaths by routing and assigning wavelength to each connection is called **Routing and Wavelength Assignment (RWA)** [30]. Routing and wavelength assignment are critically important to increase the efficiency of optical networks [31]. Typically, connection requests may be of three types: **static**, **incremental**, and **dynamic**. With static traffic, the entire set of connections is known in advance, and the problem is then to set up lightpaths for these connections in a global fashion while minimizing network resources utilization such as the number of wavelengths or the number of fibers in the network. In the incremental traffic case, connection requests arrive sequentially, a lightpath is established for each connection, and the lightpath remains in the network indefinitely. For the case of dynamic traffic, a lightpath is set up for each connection request as it arrives, and the lightpath is released after some finite amount of time. The objective in the incremental and dynamic traffic cases is to set up lightpaths and to assign wavelengths in a manner that minimizes the amount of connections blocking, or maximizes the number of connections that are established in the network at any time. This problem is referred as Dynamic Lightpath Establishment problem. It can easily be shown that the optimal RWA problem is NP-complete by using results of [30] on static lightpath establishment and by restricting the general problem to tree topologies. An integer programming formulation of the optimal RWA problem in the presence of deterministic traffic can be found in [32], while in [33] a similar formulation combined with randomized rounding has been presented.

We distinguish between static and dynamic lightpaths, depending on the nature of the traffic in the network. When the nature of traffic pattern is static, a set of lightpaths is established all at once that remain in the network for a long period of time. Such static lightpath establishment is relevant in the initial design and planning stage and the objective is to maximize the network throughput (i.e., maximize the number of lightpaths established for a given network resources). For the dynamic traffic scenario where the traffic pattern changes rapidly, the network has to respond to traffic demands quickly and economically. In such a dynamic traffic case, a lightpath is set up for each connection request as it arrives, and the lightpath is released after some finite amount of time.

2.4.2 Load Balancing

While shortest path routes may be most preferable, this choice may have to be sometimes sacrificed, in order to allow more lightpaths to be set up. Thus, RWA algorithms generally allow several alternative routes for each lightpath that needs to be established. Lightpaths that cannot be set up due to constraints on routes and wavelengths are said to be blocked, so the corresponding network optimization problem is to minimize this blocking probability. In communication networks, load balancing is a much desired feature of routing policies. Load balancing consists in distributing the load as much as possible on the network in order to delay the occurrence of congestion [34]. Network congestion is related to delay in packet switching networks, and therefore reducing congestion implies better quality of service guarantees. In networks based on circuit switching, reducing congestion means that a certain number of spare wavelengths are available on every link to accommodate future connection requests or to maintain the capability to react to faults in restoration schemes. In addition, reducing congestion means reducing the maximum traffic load on the electronic routers connected to the fibers. Load balancing distributes the load as much as possible on the network in order to delay the occurrence of congestion.

It can be noticed that for safety reasons, most of the communication networks are at least two connected (i.e. there is at least two distinct paths between each pair of nodes), and thus load balancing can (and should) be applied at most of time. QoS routing can naturally generate load balancing as the load is likely to be split on the different available paths if they feature different QoS characteristics. An overview of the benefits of this traffic separation can be found in [35]. But the links of a network are all more or less equivalent and thus a true separation of the load based on the differentiated services provided by the links is not possible. As it is also hard to solve a multi-flow problem before hand for each possible traffic fed to the network, we have to rely on adaptive load balancing, that is, balancing the load on the network according to the current state of the network.

2.5 Quality of Protection (QoP)

Similar to the concept of QoS, the protection classes are termed "**Reliability of Service**" classes [36]:

(a) **Guaranteed Protection**. The traffic will be protected by the transport layer with high probability (usually 99.999%);

(b) **Best Effort Protection**. Traffic uses less protection bandwidth than the full quantity;

(c) **Unprotected Traffic**. The transport layer does not make an effort to protect the connection if a failure occurs;

(d) **Preemptable Traffic**. This traffic usually uses protection bandwidth for classes (a) and (b), and is preempted when the bandwidth is needed by traffic class (a) or (b) to protect against a failure.

Classes (a), (c), and (d) are well defined, and their implementation has been widely studied. However, the grade of service for the best effort class (b) is seldom quantified. In [9], Ornan Gerstel and Galen Sasaki introduced an important concept: **Quality of Protection (QoP)**. Upon a failure, the probability of a connection to survive the failure is determined by its QoP. The QoP concept provided a uniform framework for all protection classes. The QoP grade $Q(C)$ of a connection C ranges from -1 to 1 to map as follows to the different protection class:

Table 2.3 QoP Grade of Different Protection Class

Protection Service	Protection Grade
(a) guaranteed	$Q(C) = 1$
(b) best effort	$0 < Q(C) < 1$
(c) unprotected	$Q(C) = 0$
(d) preemptable	$-1 \le Q(C) < 0$

$Q(C) \geq 0$ means that the connection is survivable, while $Q(C) < 0$ means that the connection is preemptable. The QoP grade $Q(C)$ is mapped into protection guarantees as follows [9]:

The probability that a connection C will survive a failure on its working path is at least $SP(C)$, which is defined to be $SP(C) = Max\{Q(C),0\}$. $SP(C)$ will be referred to as the survivability probability. If $SP(C) >$ 0, then the connection is a survivable connection.

The probability that a connection C will be preempted when there is a fault that is not on its working path is at most $PP(C)$, which is defined to be $PP(C) = Max\{-Q(C),0\}$. If $PP(C)$ will be referred as preemptable probability. If $PP(C)$ > 0, then the connection is a preemptable connection. Thus a connection C survives according to $SP(C)$ and is preempted according to $PP(C)$ when fault occurs.

In the above probabilistic schemes, survivable connections share protection bandwidth by using randomization. This is the only bandwidth sharing possible for a truly transparent optical network that carries different signal formats and is not even aware of their exact bit rates, since either a connection is completely recovered or not recovered at all. Other optical networks do have access to the carried formats, and can even multiplex/demultiplex them onto a single wavelength using **Time Division**

Multiplexing (TDM) techniques. This allows for a deterministic QoP model, whereby upon a failure, each survivable connection is guaranteed to have a deterministic reduced protection bandwidth $RPB(C) = SP(C) \cdot B(C)$, where $B(C)$ is the working bandwidth of the connection. [9] discussed the necessary and sufficient bandwidth when QoP concept is deployed in ring networks.

2.6 Problem Formulation

In this thesis, the performance of shared path protection with QoP concept in a mesh network is studied. Given the physical network topology, traffic demands and their QoP grades, the objective is to minimize the total number of wavelengths on the links in the network. Since load balancing is an important metric to evaluate the performance of optical networks, we also try to achieve load balancing while routing and assigning wavelengths for the traffic demands.

We assume that the OXC node in the optical layer can add and drop any wavelengths, i.e., an OXC node has sufficient transmitters and receivers. The topology of the optical layer can be represented by a directed graph: each vertex of the graph representing one OXC node in the optical layer, and each link in the graph representing two directed physical connections (fibers) in the optical layer.

A connection request, which is a demand for a wavelength service, has the following attributes:

- It starts from a source OXC node and terminates at a destination OXC node.
- It requires a fixed bandwidth (in unit of wavelength).
- It requires shared path protection, and has a QoP grade in the range from 0 to 1. Deterministic QoP model [8], which means each survivable connection is guaranteed to have a deterministic reduced protection bandwidth, is applied for each connection request according to its QoP grade.

The problem can be formulated as follows:

Notations:

- V : Set of N nodes.
- E : Set of L links.
- $G(V, E)$: A directed graph that represents the network topology.
- (i, j) : A link of $G(V, E)$, where $(i, j) \in E$.
- W : Maximum number of wavelengths per link.
- $B_l(s, d)$: Working bandwidth requirement in units of wavelength capacities of the l-th connection request between the source node s and the destination node d. Note that for each source-destination pair (s, d), one or more connection requests exist. We assume the maximum number of connection requests between the same source-destination pair is M. We also assume that the working bandwidth $B_l(s, d)$ of each connection request is 1 wavelength.

- $Q_l(s,d)$: QoP grade of the l-th connection request between the source node s and the destination node d. Each $Q_l(s,d)$ maps $B_l(s,d)$ uniquely, and is a real number between 0 and 1.
- C: Traffic demand matrix { $c_l(s,d)$ }, where each $c_l(s,d)$ is a combination of $B_l(s,d)$ and $Q_l(s,d)$.
- $X_{i,j}^{s,d,l}$: Bandwidth of the primary path for the l-th connection request between node pair s - d on link (i,j). Obviously $X_{i,j}^{s,d,l} = B_l(s,d)$ for each link (i,j).
- $Y_{i,j}^{s,d,l}$: Bandwidth of backup path for the lth connection request between node pair s - d on link (i,j). $Y_{i,j}^{s,d,l} = B_l(s,d) \cdot Q_l(s,d)$ for the connection requests with $Q_l(s,d) > 0$, $Y_{i,j}^{s,d,l} = 0$ for the other connection requests.
- $\delta_{i,j,k}^{s,d,l}$: A binary value. $\delta_{i,j,k}^{s,d,l}$ is 1 if the wavelength k on the link (i,j) is used by a path (primary path or backup path) for the l-th connection request between the source node s and the destination node d. $\delta_{i,j,k}^{s,d,l}$ is 0 otherwise.
- R = { $r_{i,j}^m$ }: A set of $L-1$ sub-groups associated with link (i,j). Each member of R, i.e. $r_{i,j}^m$ (m =1, 2,…, L -1), represents the set of all the connection requests that share same links. This means that the connection requests belonging to the m-th sub-group $r_{i,j}^m$ may fail simultaneously, when failure occurs on the m-th link in the network. Because there are L links in the network, so the number of the members of R is L -1.

- $w_{i,j}$: Number of wavelengths used on link (i,j) , and is given by $w_{i,j} = \left\lceil \sum_{c_l(s,d)\in C} X_{i,j}^{s,d,l} + \max_{r_{i,j}^m \in R}\{ \sum_{c_l(s,d)\in r_{i,j}^m} Y_{i,j}^{s,d,l} \} \right\rceil$, where $\lceil a \rceil$ denotes the least integer that is more than or equal to a . For each m (1, 2, … , $L-1$), $\sum_{c_l(s,d)\in r_{i,j}^m} Y_{i,j}^{s,d,l}$ represents the bandwidth required on link (i,j) to provide protection for the m-th link (i.e., the m-th subgroup). Because shared path protection is used in our algorithm, the maximum sum of bandwidth required among the $L-1$ subgroups is enough to provide protection.

The objective is

$$\text{minimize} \quad \sum_{(i,j)\in E} w_{i,j}$$

Subject to:

Flow conservation at each node:

For the primary path, the input traffic and output traffic are the same at any intermediate node among the paths for any $s-d$ pair. For any source node s , the input traffic is 0 such that the total traffic through node s equals to the bandwidth requirement of traffic leaving s . Similarly, for the destination node d , the output traffic is 0 such that the total traffic at node d equals to the bandwidth requirement of traffic terminating at d . So we get:

$$\sum_{\forall i:(i,s)\in E} X_{i,s}^{s,d,l} = 0 , \qquad \forall s \in V, 1 \le l \le M, 1 \le w \le W$$

$$\sum_{\forall j:(d,j)\in E} X_{d,j}^{s,d,l} = 0 , \qquad \forall d \in V, 1 \le l \le M, 1 \le w \le W$$

$$\sum_{i:(i,j)\in E} X_{i,j}^{s,d,l} - \sum_{k:(j,k)\in E} X_{j,k}^{s,d,l} = \begin{cases} -B_l(s,d), & j = s \\ B_l(s,d), & j = d \\ 0, & otherwise \end{cases} \qquad \forall j, s, d, l \, .$$

For the backup paths, the input traffic and out put traffic at intermediate node are also same. However, at the source nodes and destination nodes, the amount of out put traffic is determined by both the primary bandwidth ($B_l(s,d)$) and the QoP grade ($Q_l(s,d)$)of the demand.

$$\sum_{i:(i,j)\in E} Y_{i,j}^{s,d,l} - \sum_{k:(j,k)\in E} Y_{j,k}^{s,d,l} = \begin{cases} -B_l(s,d)\cdot Q_l(s,d), & j=s \\ B_l(s,d)\cdot Q_l(s,d), & j=d \\ 0, & otherwise \end{cases} \quad \forall j,s,d,l\,.$$

$$\sum_{\forall i:(i,s)\in E} Y_{i,s}^{s,d,l} = 0\,, \qquad \forall s \in V, 1 \le l \le M, 1 \le w \le W$$

$$\sum_{\forall j:(d,j)\in E} Y_{d,j}^{s,d,l} = 0\,, \qquad \forall d \in V, 1 \le l \le M, 1 \le w \le W$$

Link disjoint constraint between primary paths and back paths:

Primary paths and backup path for any $s-d$ connection demand cannot share any link in the network. So for each link (i,j), one of $X_{i,j}^{s,d,l}$ and $Y_{i,j}^{s,d,l}$ has to be 0, so we get:

$$X_{i,j}^{s,d,l} + Y_{i,j}^{s,d,l} \le \max\{X_{i,j}^{s,d,l}, Y_{i,j}^{s,d,l}\} \;\; \forall (i,j)\in E \;\; \text{and} \;\; \forall s,d \in V$$

Link capacity constraint:

For all the demands whose backup path goes through link (i,j), the maximum backup bandwidth among the sub-groups ($\max_{r_{i,j}^m \in R}\{\sum_{c_l(s,d)\in r_{i,j}^m} Y_{i,j}^{s,d,l}\}$) is assigned as the backup bandwidth for all the demands. Because the primary paths for all the sub-groups and the backup path are link disjoint, this bandwidth is enough to provide protection. The total bandwidth of primary paths ($\sum_{c_l(s,d)\in C} X_{i,j}^{s,d,l}$) and backup paths ($\max_{r_{i,j}^m \in R}\{\sum_{c_l(s,d)\in r_{i,j}^m} Y_{i,j}^{s,d,l}\}$) should be smaller than the capacity of the link (i,j), i.e., W

$$w_{i,j} = \left\lceil \sum_{c_l(s,d)\in C} X_{i,j}^{s,d,l} + \max_{r_{i,j}^m \in R}\{\sum_{c_l(s,d)\in r_{i,j}^m} Y_{i,j}^{s,d,l}\} \right\rceil \le W \quad \text{for} \quad \forall (i,j)\in E$$

For networks without wavelength convertibility, *wavelength continuity constraint*:

For any intermediate node j, if the input link (i, j) uses wavelength k for l-th demand between $s-d$, the output link (j,e) used for this demand must be assigned wavelength k to ensure wavelength continuity.

$$\sum_{\forall i:(i,j)\in E} \delta_{i,j,k}^{s,d,l} - \sum_{\forall e:(j,e)\in E} \delta_{j,e,k}^{s,d,l} = 0 \quad \forall s,d \in V\,, \quad \forall j \in V : j \neq s \quad \text{and} \quad j \neq d\,, \quad 1 \leq k \leq W$$

Chapter 3: Provisioning in Networks with Wavelength Converters

The formulations presented in Chapter 2 are similar to **Integer Linear Programming (ILP)** [37] formulations except that the protection bandwidth required by the connection requests is a real number. Although solving the ILP problems is still possible for some small-sized networks, it is not practical for large-sized networks. Therefore, we develop a heuristic solution for solving the provisioning problem in survivable WDM networks.

3.1 Finding k-Shortest paths

Our heuristic solution is initiated by finding a set of k-shortest paths for each connection request. These k-shortest paths are subject to the following constraints:

- Looplessness: allows for no repeated vertexes on each path.
- Link disjoint: ensures no link in any path being shared with any other one that has the same source vertex and destination vertex.

3.1.1 Problem Definition

Give a network $G(V,E)$, where $V=\{v_1,v_2,...,v_N\}$ is a finite set with N vertexes and $E=\{e_1,e_2,...,e_L\}\subseteq N\times N$ is a finite set with L edges. Sometimes we use i to represent vertex v_i for simplicity. Each edge $e_k \in E$ can also be identified by a vertex pair (i, j), where $i, j \in V$.

Let i and j be two vertexes of G. If each pair (i, j) in G is ordered, i.e., if all the edges of the network are directed, G is said to be a directed network; if all the edges are not ordered, then G is said to be an undirected network. Without loss of generality, we consider the network a directed one, since each undirected edge can be replaced by two arcs with opposite direction. It is also assumed that there is at most a single edge between each pair of vertexes of the network and there are no edges of the form (i,i), where $i \in V$.

Given $i, j \in V$, a path from vertex i to vertex j in G is an alternating sequence of vertexes and edges, of the form $p =< i = v_1, e_1, v_2, ..., e_{m-1}, v_m = j >$, where

- $v_k \in V$ for every $k \in \{1,2,...,m\}$
- $e_k \equiv (v_k, v_{k+1}) \in E$ for every $k \in \{1,2,...,m-1\}$

In order to simplify the notation, a path will be represented only by its vertexes; that is, $p =< i = v_1, v_2, ..., v_m = j >$ and for convenience, sometimes a single vertex is viewed as a path, the null path. The set of paths defined from i to j in G will be denoted by $P_{i,j}$. A loopless path from i to j is a path from i to j in which all vertexes on this path are different and a loop is a path from some vertex to itself.

Let $c_{i,j}$ be a real number associated with edge (i, j) of G, known as the cost of edge (i, j), and let $c(p) = \sum_{(i,j)\in p} c_{i,j}$, for a given path p in G, be the cost of path p.

Let s and d be two different vertexes of G, called source and destination vertex, respectively. In order to simplify the expression, P will denote set $P_{i,j}$. In what follows, with no loss of generality, it will be assumed that $P_{s,i} \neq 0$ and $P_{i,d} \neq 0$ holds, for every vertex i in G.

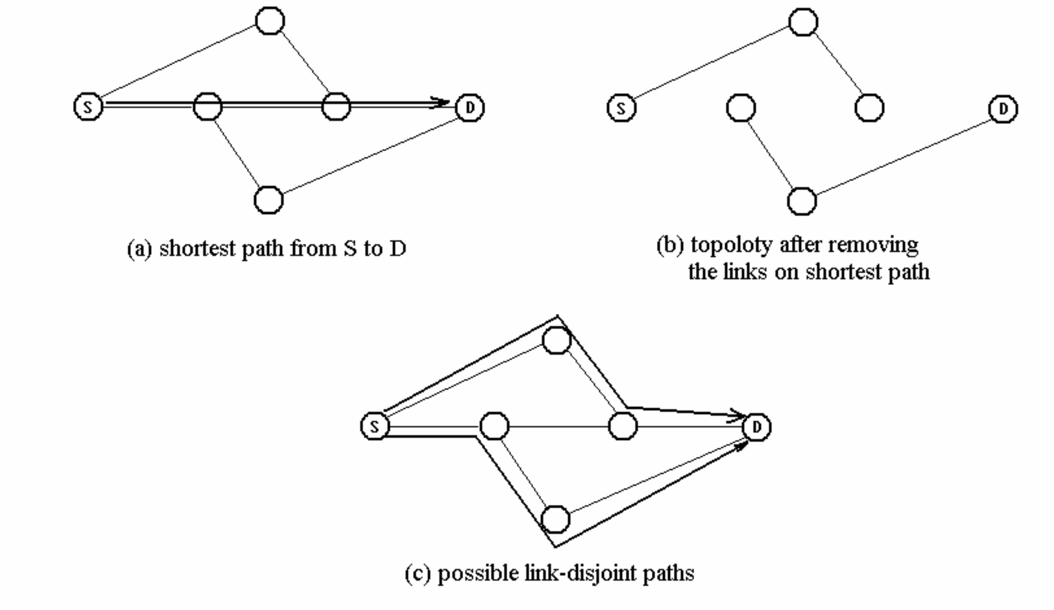
In the classical shortest path problem, it is intended to determine a path $p*$ from s to d in G with minimum cost. That is, it is intended to determine $p* \in P$ such that $c(p*) \leq c(p)$ for any $p \in P$. Given an integer $k > 1$, the k shortest paths problem can be considered a generalization of the previous one where, beyond the determination of the shortest path in P, it also has to determine the second shortest path in P, …, until the k-th shortest path in P. That is, denoting by p_i, the i-th shortest path from vertex s to vertex d in G, it is intended to determine a set of paths, $P_k = \{p_1, p_2, ..., p_k\} \subseteq P$ such that:

1. p_i is determined before p_{i+1}, for any i=1, …, k-1;
2. $c(p_i) \leq c(p_{i+1})$, for any i=1, …, k-1;
3. $c(p_k) \leq c(p)$, for any $p \in P - P_k$

Additionally, these k-shortest paths should be link disjoint.

3.1.2 k-Shortest Paths Searching

The simplest method to find k-shortest paths is to find the paths one after another. Taken $k = 2$ as an example, it is actually a two step search. In this method, a shortest path in the network connecting the source vertex and the destination vertex is found first (e.g. applying the Dijkstra algorithm), and it is allocated a working lightpath. Then the links used by the working path are removed from the network (ensuring the link disjoint constraint), and the shortest-path algorithm is run again to route the second shortest path, which is assigned the protection lightpath. This method is greedy: there is situation in which it fails to find the solution even if a link disjoint path pair actually exists. This situation can be illustrated by using Figure 3.1:



(a) shortest path from S to D

(b) topoloty after removing the links on shortest path

(c) possible link-disjoint paths

Figure 3.1 Routing of a Link-Disjoint Path Pair in a Trap Network

In this example, each link in the network has weight one. The connection request will be routed from the source vertex S to the destination vertex D. Figure 3.1.a shows the shortest path that is found in the first step. In Figure 3.1.b, the links that are used in the shortest path are cut from the network topology. So the second step fails to find another path from vertex S to vertex D and the protection path cannot be provided. However, there exists a link-disjoint path pair between the vertex S and the vertex D, which is shown in the Figure 3.1.c. So this method is not suitable for searching k-shortest paths in a mesh network.

A technique which is able to overcome the two-steps limitations has been proposed by Bhandari [38]. It is called one-step search, since the two lightpaths of the path pair are not routed separately, but they are jointly routed by performing a suitable algorithm (the modified Dijkstra algorithm).

3.2 Heuristic Solution for Provisioning Problem

We develop a heuristic solution for the provisioning problem in survivable WDM networks with shared path protection and QoP grades. In this solution, we do not consider the wavelength continuity constraints in the WDM network, i.e., we assume sufficient number of full wavelength converters are available at each node in the network. For this algorithm, the input is the physical network topology (WDM layer) and a set of connection requests each with a QoP grade. The objective is to provision these requests with minimum number of total wavelengths used. The algorithm is given bellow:

1. Group the connection requests according to their source and destination, i.e., the connection requests with the same source and destination belong to the same group. The connection requests are specified by the bandwidth requirement $B_l(s,d)$ and QoP grade $Q_l(s,d)$. Thus there are M such groups (i.e. M $s-d$ pairs) where M is the number of $s-d$ pairs. Connection requests in the group require different number of wavelengths and different QoP grades. Assume that the total QoP grade for each group is q_m, where $m=1,2,...,M$ and q_m is the sum of all the QoP grades whose corresponding source-destination pair belongs to the m-th group.
2. Route for an arbitrary group (say, the m-th group) in the network, i.e. find all link disjoint paths for this source-destination pair. Assume that P_m ($P_m \geq 2$) paths are found for the m-th group. If P_m is less than 2, no backup path can be found to provide protection. Then this connection request cannot be satisfied, and next connection request is taken into consideration.
3. Choose the longest path as the backup path for all the primary paths in this group. Since the wavelengths required on backup path is usually less than the wavelengths required on the primary path (due to the QoP grade), choosing the longest path as the backup path will result in shorter primary paths and help to reduce the total number of wavelengths used in the network.
4. If the number of the connection requests (with the same source and destination), say S_m, is less than or equal to $P_m - 1$ (one path has to be reserved for backup path, so only $P_m - 1$ paths can be used as primary paths), go to step 5. If the

number of connection requests is larger than $P_m - 1$, merge the connection requests of this group (the m-th group) into $P_m - 1$ sub-groups. Here we still use S_m to denote the number of sub groups, i.e., $S_m = P_m - 1$. During merging, three principles are applied: (a) keep the total number of wavelengths required by each sub-group as few as possible. (b) no sub-group requires significantly more wavelengths than the others. (c) the sum of the QoP grades in each sub-group is closer to some integer. Let Q_m^s be the sum of the QoP grades in sub-group s of the m-th source-destination pair. Obviously, $S_m \le P_m - 1$, and $\sum_{s=1}^{S_m} Q_m^s = q_m$.

5. Allocate the S_m sub-groups one by one to the unused $P_m - 1$ paths (just allocate paths, and assign wavelengths later in Step 6). Choose the S_m shortest paths as the primary paths and assign wavelengths to these paths. If $S_m < P_m - 1$, at least one path is free so that the originally reserved backup path can be moved to a shorter one. This makes the total number of wavelengths used in the network as small as possible.
6. Assign wavelengths for primary paths and backup paths. The wavelength for the primary path is the wavelength requirement of each connection request, and the wavelength for backup path is $W_s = \left| \max\{Q_m^s\} \right|$, where $\lceil a \rceil$ denotes the least integer greater than or equal to a real number a.
7. Assign routes and wavelengths for the remaining groups of with the same method by repeating step 2 through step 6 for each of these groups.
8. If the number of wavelengths on some link is much higher than the one on the other links (i.e., load balancing is not achieved), re-allocate routes and wavelengths

for all the connections. Compare the result with the previous one. After some times, select the most satisfactory result.

The flowchart of this algorithm is shown in Figure 3.2.

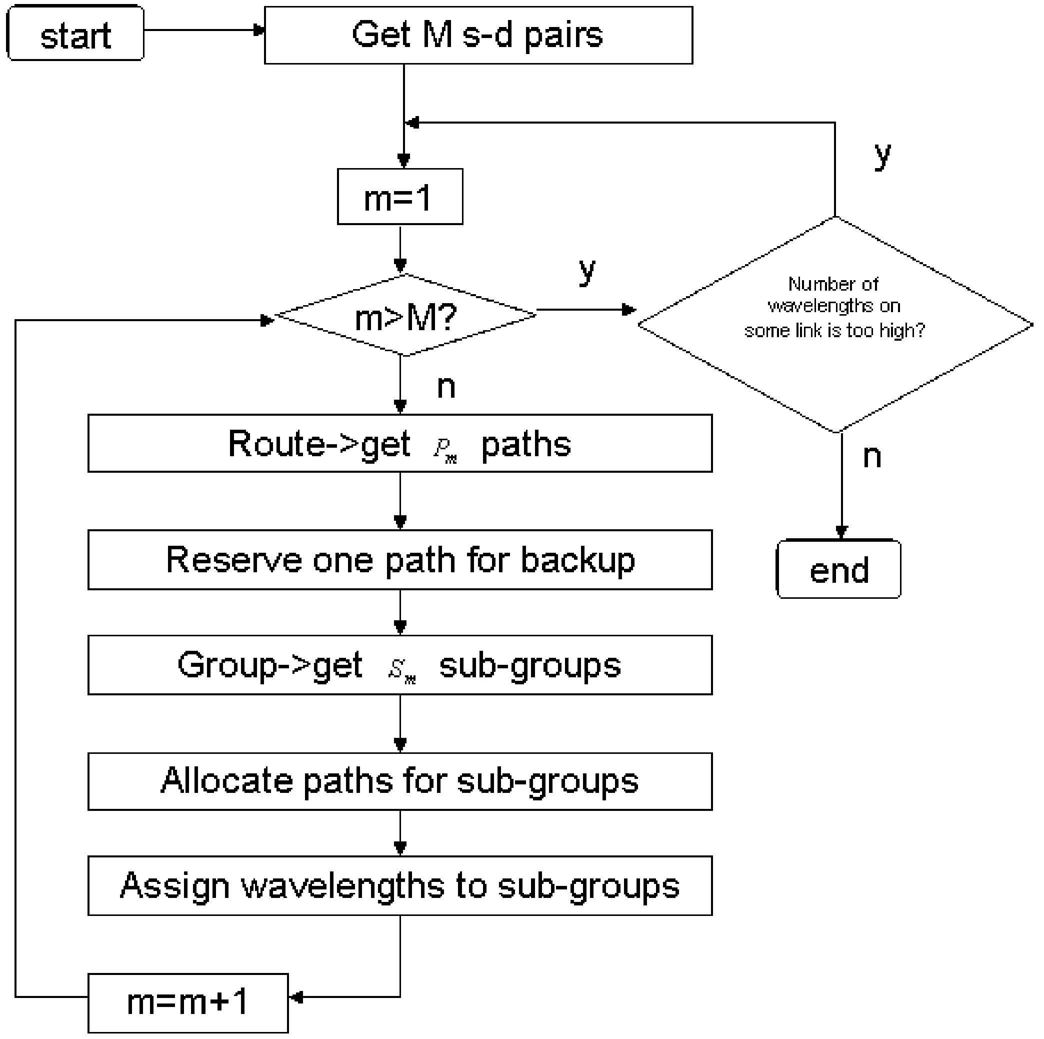

start
Get M s-d pairs
m=1
m>M?
y
n
Number of wavelengths on some link is too high?
y
n
end
Route->get P_m paths
Reserve one path for backup
Group->get S_m sub-groups
Allocate paths for sub-groups
Assign wavelengths to sub-groups
m=m+1

Figure 3.2 Heuristic Algorithm

The following is an example to illustrate how this heuristic method works. Consider the network shown in Figure 3.3. There are two $s-d$ pairs: one is (1, 4) with four demands, the other is (2, 4) with three demands. The bandwidth and QoP requirement is shown in Table 3.1.

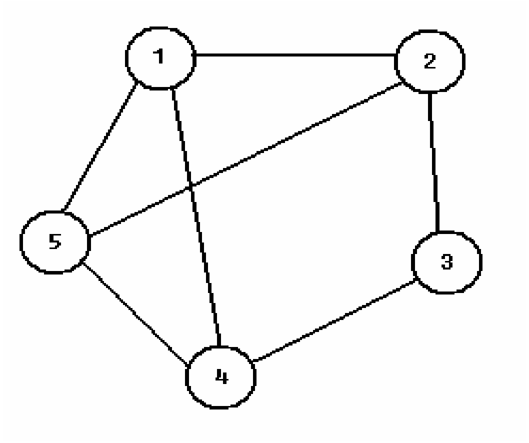


Figure 3.3 Physical Network Topology

Table 3.1 Demands and Their QoP Grades

s-d pair	**demand**	$B_l(s,d)$	$Q_l(s,d)$
(1, 4)	1	1	0.7
	2	1	0.5
	3	1	0.4
	4	1	0.3
(2, 4)	1	1	0.5
	2	1	0.3
	3	1	0.1

First, assign route and wavelength for $s-d$ pair (1, 4). Three link disjoint paths have been found with the k-shortest paths algorithm described previously: (i) 1->4, (ii) 1->5->4, and (iii) 1->2->3->4. We choose the longest path (i) as the backup path and the other two as the primary paths. Because there are four correction requests from node 1 to node 4, while there are only two paths reserved for the primary paths, we group these connection requests into sub-groups. According to the QoP grades, these requests are merged into two sub-groups. According to the principles described in the algorithm, request 1 and 4 are merged into one sub-group, and request 2 and 3 are merged into the other one. Then the number of wavelengths required in backup path is $\lceil \max\{0.7+0.3, 0.5+0.4\} \rceil = 1$. Obviously, there are other choices of grouping these four requests. For example, we can merge request 1 and 2 into one sub-group, and request 3 and 4 into another one. In this case, the wavelengths used in the two primary paths are the same as the previous case. However, the number of wavelengths in the backup path is changed to $\lceil \max\{0.7+0.5, 0.4+0.3\} \rceil = 2$. This sub-grouping method is not what we need, because it consumes more wavelengths for the backup path.

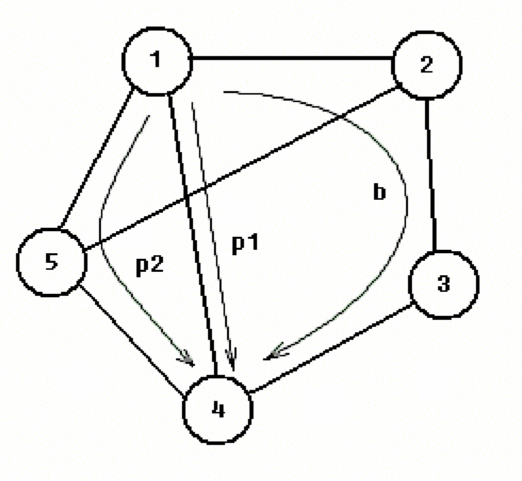


Figure 3.4 Paths from Node 1 to Node 4

There are three link disjoint paths for $s-d$ pair (2, 4). The link disjoint paths are found: (i) 2->1->4, (ii) 2->5->4, and (iii) 2->3->4. After reserving path (ii) as the backup path, the other two can be used as the primary paths. Of course we can use one of the two paths as the primary path. In this case, the primary path consumes 3 wavelengths on each link along the path, and one wavelength on the backup path ($\lceil 0.5+0.3+0.1 \rceil = 1$). However, this results in bad load balancing in the network. No matter how we choose the primary paths and the backup path, at least one link in the network will use up to 4 wavelengths, because the connection requests from 1 to 4 have consumed some wavelengths on some of the links. So we choose both of the two paths as primary paths. In Figure 3.5, path p1 is assigned two wavelengths for the connection requests with QoP of 0.3 and 0.1, and path p2 is assigned one wavelength for the connection request with QoP of 0.5. In this case, the number of wavelengths on backup path b is still $\lceil \max\{0.1+0.3, 0.5\} \rceil = 1$.

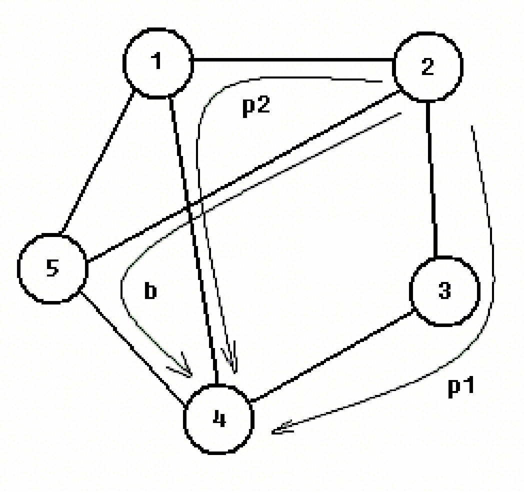


Figure 3.5 Paths from Node 2 to Node 4

After assigning route and wavelength for all the connection requests, the wavelength usage in the network is as shown in Figure 3.6:

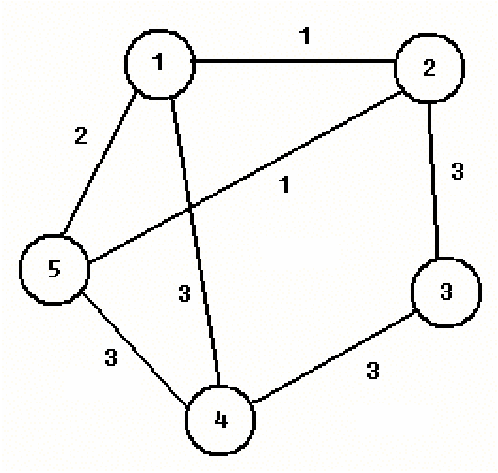


Figure 3.6 Wavelength Usage after RWA

Now, steps from 2 to 7 in the algorithm have been completed. This result may not be the best result for the given connection requests, taken into consideration of wavelength usage and load balancing. So some connection can be rerouted or reconfigured. This is what step 8 does. We will compare the simulation results of wavelength usage and load balancing before and after reconfiguration in the following part.

The main components in our algorithm are finding k-shortest paths, sub-grouping the connection requests with same source node and destination node, and assigning wavelengths for each path. For each connection request, the complexity of the modified Dijkstra algorithm we used for searching k-shortest paths is $O(N^2)$ [38], where N is the number of the number of the nodes in the network. Sub-grouping connection requests and assigning wavelength take much less time, and the complexity of these two parts is proportional to the number of link-disjoint paths between the source node and destination node of the connection request. So finding the k-shortest paths for each $s-d$ pair is the most time consuming part of our algorithm. Since there are $N \times N$ $s-d$ pairs, the complexity of our algorithm is $O(N^4)$. Searching k-shortest paths is also the one of most important parts in our algorithm. The more link-disjoint paths we can find, the more efficiently the wavelengths can be utilized. Another key component of our algorithm is sub-grouping. It directly determines how the wavelengths are assigned to each path, as described in the above examples.

3.3 Simulation Results

To verify our heuristic algorithm, we conduct simulation on two different mesh networks: a small-sized network with 8 nodes and 16 bi-directional links (shown in Figure 3.7), and ARPANET with 16 nodes and 32 links (shown in Figure 3.8).

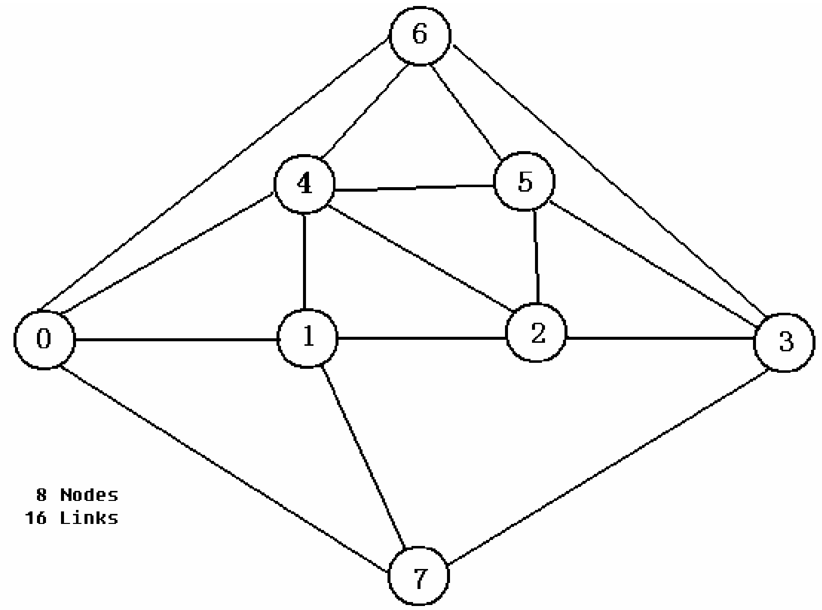


Figure 3.7 The 8-Node Simulation Network

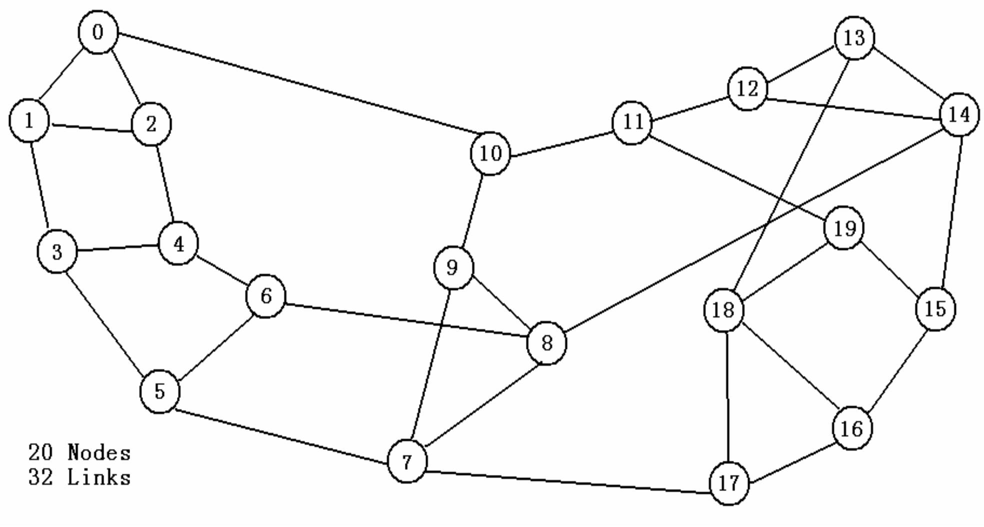


Figure 3.8 ARPANET

3.3.1 Network Topologies and Traffic Model

In these two networks, each link represents two unidirectional fiber links in opposite directions. In the simulation, each node can be a source node and destination node. For a source node in the network, all the other nodes in the network are destination nodes with equal probability. The connection requests between each such source-destination pair are generated randomly according to a uniform distribution. We set the maximum number of requests between each source-destination pair to 5 such that the average number of connection requests between any source-destination pair is around 3. Each connection request is assigned a QoP grade. The simulation is conducted according to the average QoP grade of the connection requests. We select the QoP grade according to a uniform distribution. For an average QoP grade of 0.3, the QoP grades are evenly distributed with the range of (0.0, 0.6). When the average QoP grade of the connection requests is 1.0, i.e., the QoP grade of each connection request is 1.0, and only shared path protection is applied in this simulation.

3.3.2 Minimizing Total Number of Wavelengths Used

Our objective is to minimize the total number of wavelength consumed by all the connection requests. We compare the wavelength usage of our solution with the one of the dedicated full protection scheme. In dedicated full protection scheme, each primary path is assigned a dedicated link disjoint backup path. Figure 3.9 shows the wavelength usage in the 8-node network:

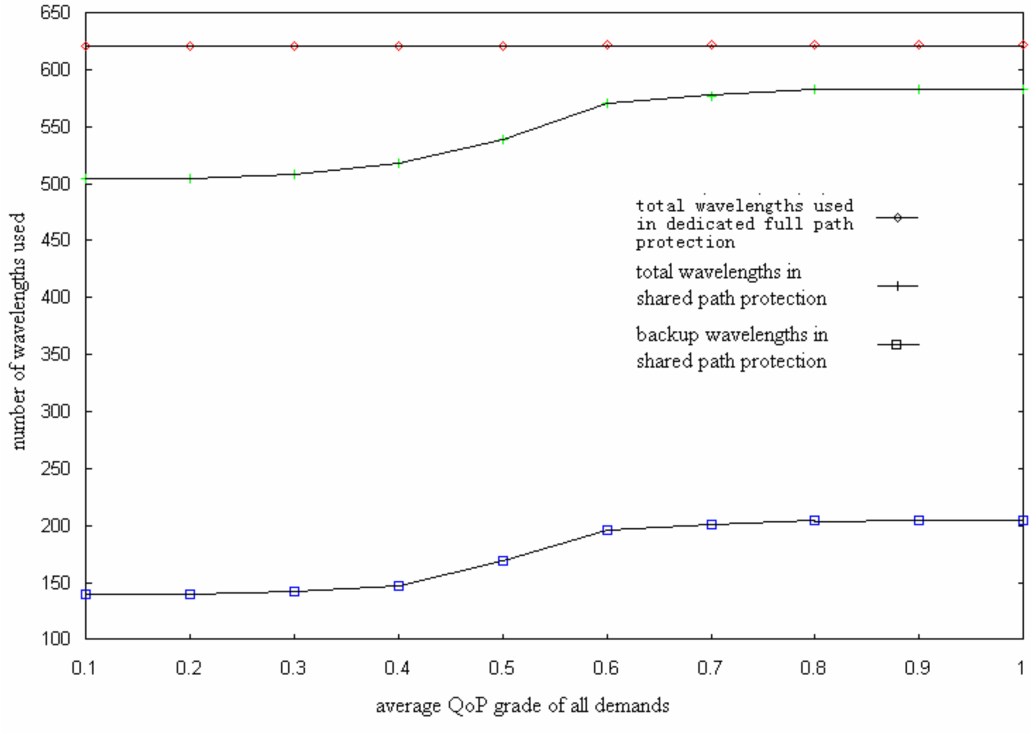


Figure 3.9 Wavelength Usage in the 8-Node Network

In the simulation, totally 178 connection requests are generated. The number of wavelengths consumed by primary paths is not shown in this figure, because it does not change significantly (from 356 to 372) as QoP grade increases from 0.1 to 1.0.

From Figure 3.9, it can be observed that as the average QoP grade increases from 0.1 to 1.0, the number of wavelengths consumed by backup paths changes from 149 to 221. This number increases slowly as the average QoP grade increases. The total number of wavelengths (the sum of wavelengths consumed by both the primary paths and the backup paths in shared path protection) changes from 504 to 581 with almost the same tendency. The number of wavelengths used by the dedicated full path protection is always the same value even though the average QoP grade of the connection requests is not always same in the simulation. This is because each connection is given a dedicated backup path with full protection and QoP grade has no meaning here.

The wavelength usage changes a little when the average QoP grade is within the lower end or the higher end of the coordinate, while it increases at a fast rate when the average QoP grade falls in the range from 0.4 to 0.7. As the average QoP grade increases from 0.1 to 0.3, the number of wavelengths used by the backup paths increases from 149 to 152. Within the range from 0.8 to 1.0, the number of wavelengths used by the backup paths remains unchanged (211). Because we do not allow wavelength sharing among different connection requests (from different source or destination), the sharing efficiency is mainly achieved by grouping the connection requests with same source and destination nodes. When the average QoP grade is low, say 0.2, the QoP grade of each connection request ranges from 0 to 0.4, because these QoP grades are selected with uniform distribution. Additionally, the average number of connection requests between each source-destination pair is 3 such that only a few of the source-destination pairs need more than one wavelength for protection. That is why the number of wavelengths for backup paths does not change much when the average QoP grade is low. The similar reason can also give the explanation to why the number of wavelengths consumed by backup paths does not change when the average QoP grade is high. Fast change occurs when the average QoP grade is in the range from 0.4 to 0.7. This fact is due to the various combination results for the backup lightpath among the same source-destination pair. When the average QoP grade reaches 1.0, the total number of wavelengths consumed by both the primary paths and the backup paths is close to the one consumed in dedicated full path protection. In our protection solution scheme, two factors affect the bandwidth usage in the network. One is the QoP grade of the connection requests, because it makes partial protection possible. The other one is the sharing among backup paths with the same source-destination nodes. When the average QoP grade reaches 1.0, the affect of QoP grade disappears, and only backup path sharing is effective in saving the bandwidth and so the wavelengths are minimally saved.

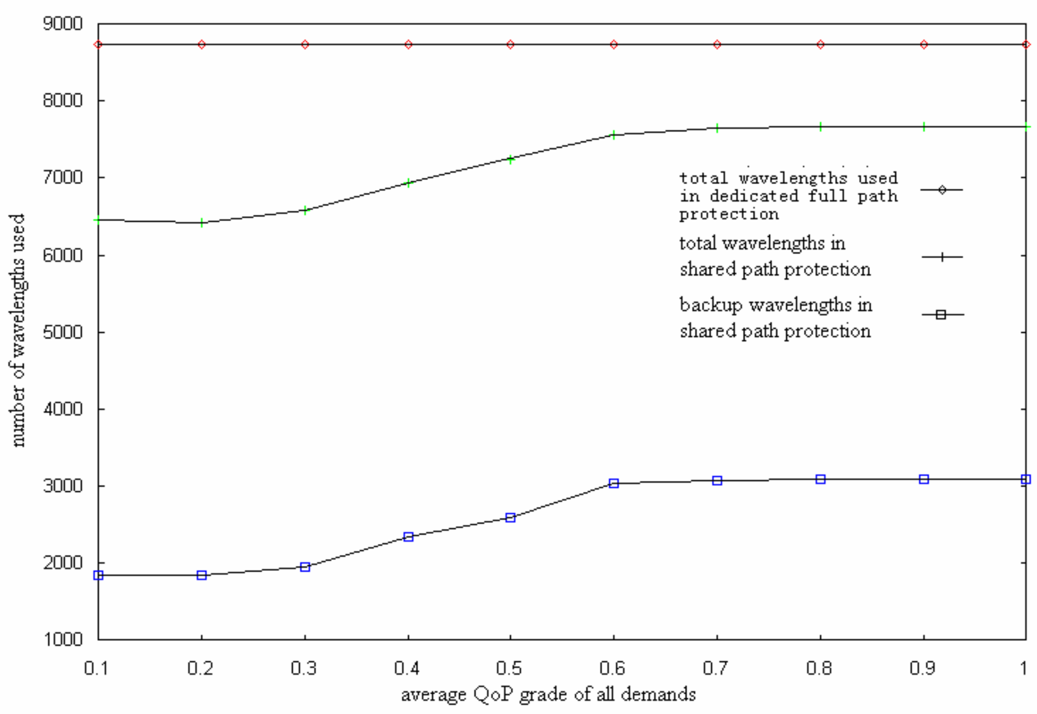


Figure 3.10 Wavelength Usage in ARPANET

Figure 3.10 shows the simulation results of wavelength usage in ARPANET. In this simulation, 1159 connection requests were generated. These results are similar to those of the previous network.

3.3.3 Load Balancing in Networks

Load balancing is an important metric in our simulation. In real networks, the number of wavelengths on each link should be same. Hence, given the static traffic demands, the maximum number of wavelengths per link is a key parameter in network design.

Necessity of Rerouting

Figure 3.11 shows the wavelength usage per link in the 8-node simulation network.

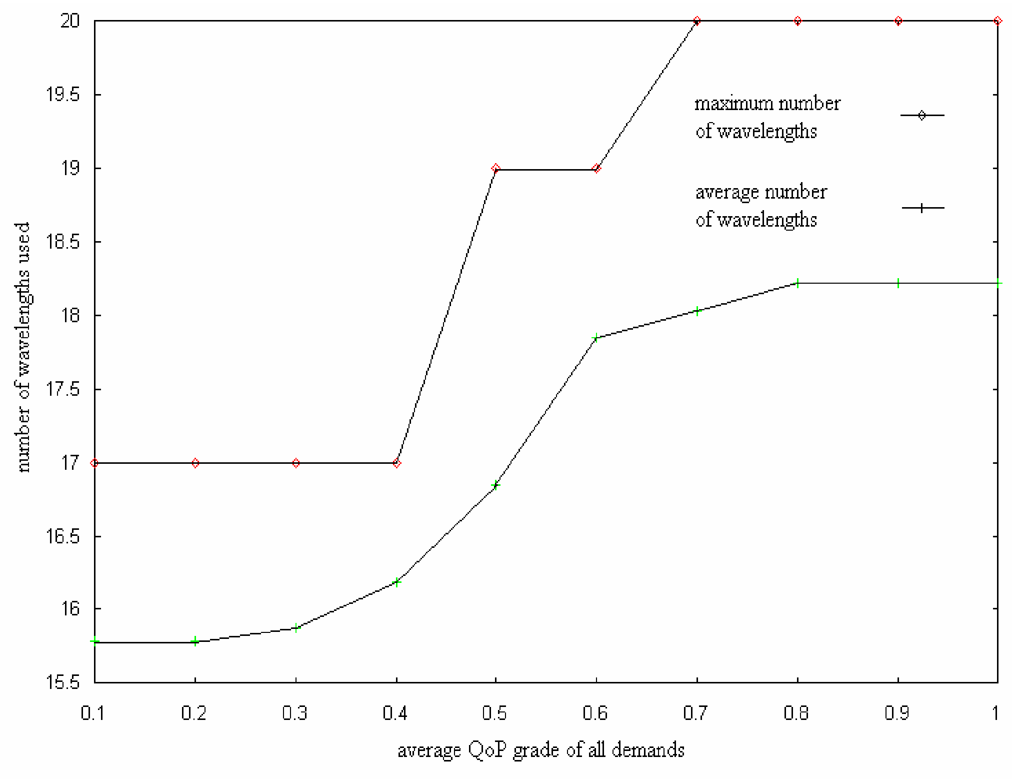


Figure 3.11 Wavelength Usage per Link in the 8-Node Network

As shown in the figure, the trend of maximum number of wavelengths per link is similar to that of average number of wavelengths per link. The maximum number of wavelengths per link is about 2 wavelengths more than the average number of wavelengths per fiber. The largest difference occurs when the average QoP grade is 0.5. At this point, the average number of wavelengths per link is 16.84, while the maximum number of wavelengths in the network is 19, about 12.83% higher than the average one. The minimum difference is only 5.02% which occurs when the average QoP is 0.4. This is an acceptable result. Rerouting played a key role in achieving load balancing in this simulation. After rerouting, the average number of wavelengths per link fluttered somehow compared with the one before rerouting. However, the maximum number of wavelengths used in the network reduced. Table 3.2 illustrates the difference of the wavelengths required before and after rerouting.

Table 3.2 Compare of Results Before and After Rerouting

Average QoP Grades	**Average Wavelengths per Link**		**Maximum Wavelength in Network**	
	before rerouting	after rerouting	before rerouting	after rerouting
0.1	15.09375	15.78125	21	17
0.2	15.09375	15.78125	22	17
0.3	15.18750	15.87500	23	17
0.4	15.50000	16.18750	25	17
0.5	16.15625	16.84375	26	19
0.6	17.15625	17.84375	26	19
0.7	17.40625	18.03125	28	20
0.8	17.53125	18.21875	29	20
0.9	17.53125	18.21875	29	20
1.0	17.53125	18.21875	29	20

After rerouting, the average number of wavelengths is a little higher than the one before rerouting. However the maximum number of wavelengths used in the network decreases at each point. This is a worth tradeoff.

Network Connectivity and Load Balancing

Figure 3.12 shows the results for ARPANET. From the results, it can be observed that the maximum number of wavelengths in the network is much higher than the average number of wavelengths per link. The largest difference occurs when the average QoP grade is 0.1, where the maximum number is 25.64% higher than the average one. The minimum difference occurs when the average QoP grade is higher than 0.7, where the maximum number is 12.68% higher than the average one. Compared with the simulation in the 8-node network, this difference is higher.

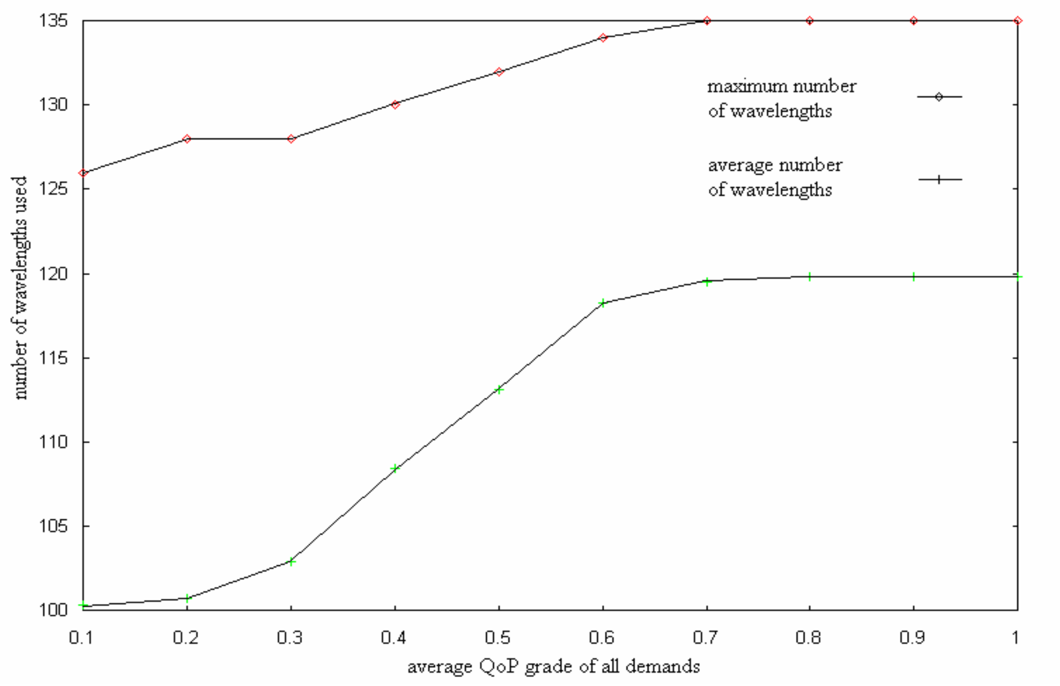


Figure 3.12 Wavelength Usage per Link in ARPANET

Figure 3.13 and Figure 3.14 shows the heavily-loaded links (within 5% percent bellow the heaviest loaded one) in the two networks after provisioning for all the connection requests for an average QoP grade of 0.5. In the 8-node simulation network, many links carry heavy traffic load as shown in Figure 3.13. On the other hand, in ARPANET only few links carry heavy traffic as shown in Figure 3.14. This phenomenon can be explained by the network topologies. It can be seen that the 8-node network is denser than ARPANET. In the 8-node network, each node connects others through at least 3 links. Actually, only one node (node 7) connects three links, most of the others have four or more links. Such topology provides the multiple routes for the connection requests so that there are more choices to choose routes to avoid congestion. However, in ARPANET, nodes degree is small and most of them have only 3 links connecting to other nodes. The heavily loaded links are mainly distributed in the middle of the network, i.e., the links connecting the left part to the right part. Because the connection requests have to be routed through these links when the source node and the destination node are located at opposite sides of ARPANET, these links carry most of the traffic in the network.

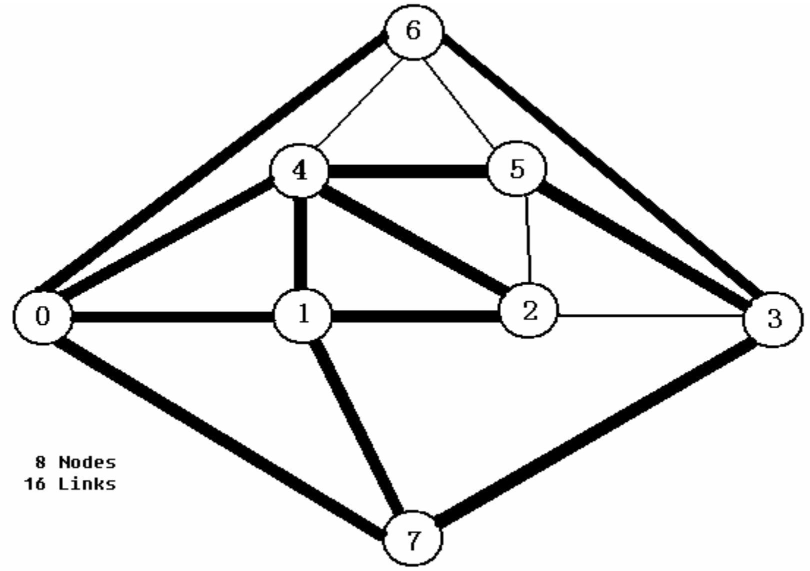


Figure 3.13 Heavily-Loaded Links in the 8-Node Network

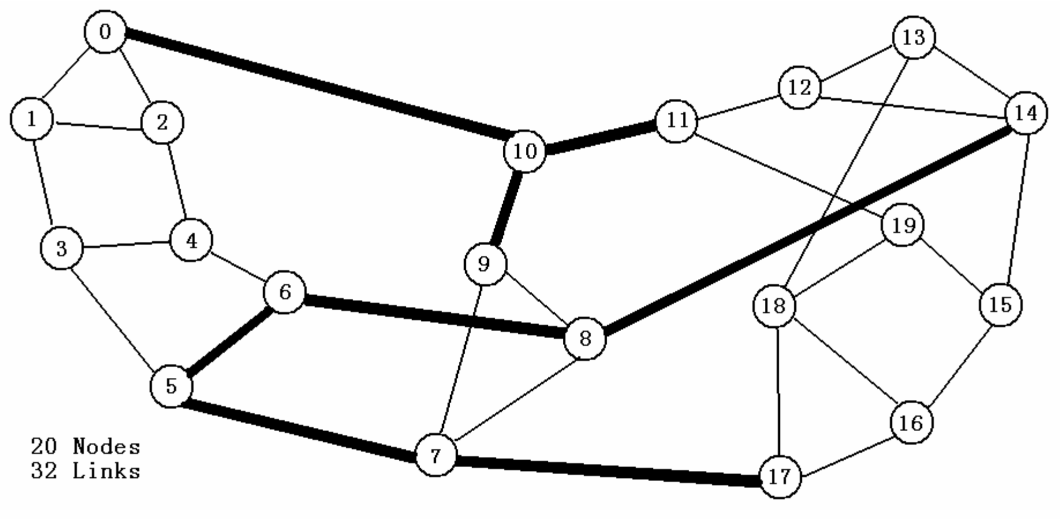


Figure 3.14 Heavily-Loaded Links in ARPANET

To verify this, we transformed the network topologies, and simulated with the same connection requests. In the 8-node network, we delete three links, i.e., (1, 4), (2, 4), and (5, 6). In ARPANET, we add six links, i.e., (0, 13), (1, 16), (2, 11), (3, 17), (4, 12), and (5, 15). The modified network topologies are shown in Figure 3.15 and Figure 3.16, respectively.

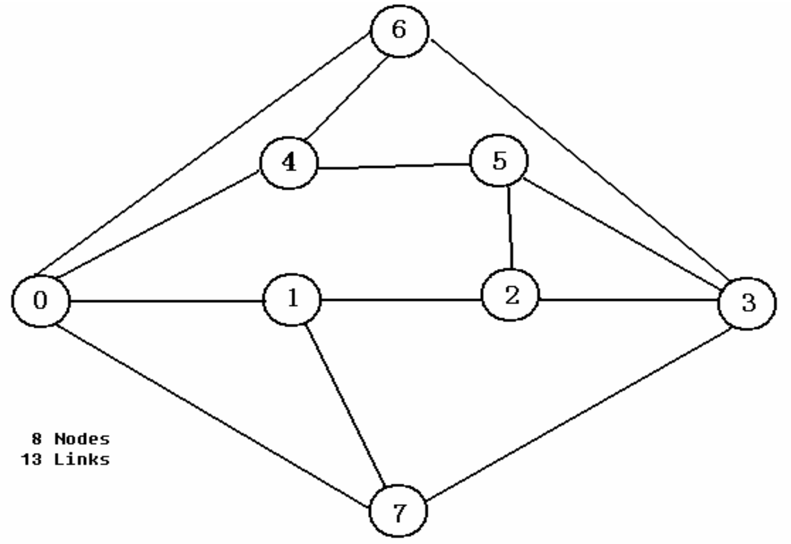


Figure 3.15 Modified 8-Node Simulation Network

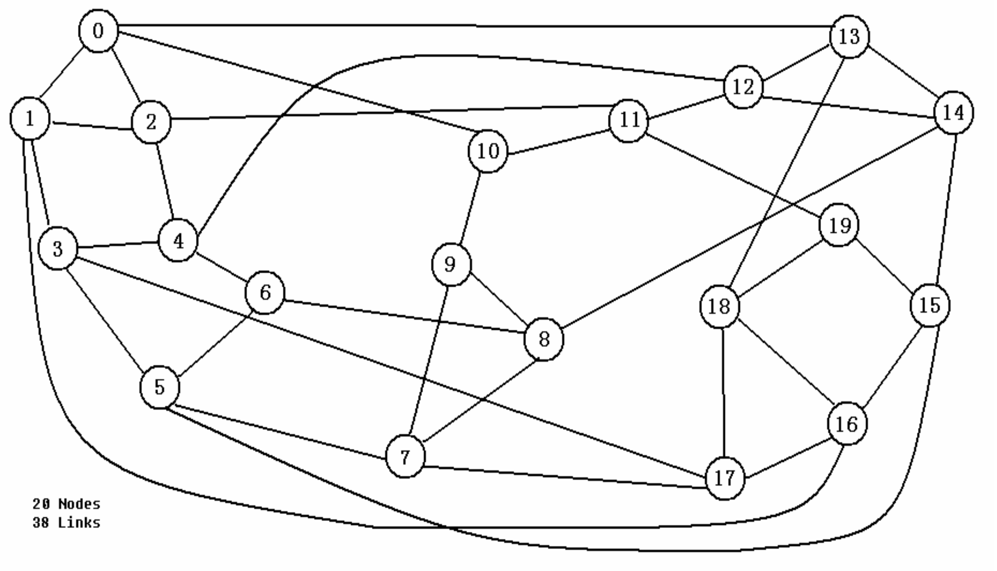


Figure 3.16 Modified ARPANET

The load balancing results after modifying the network topologies are shown in Figure 3.17 and Figure 3.18.

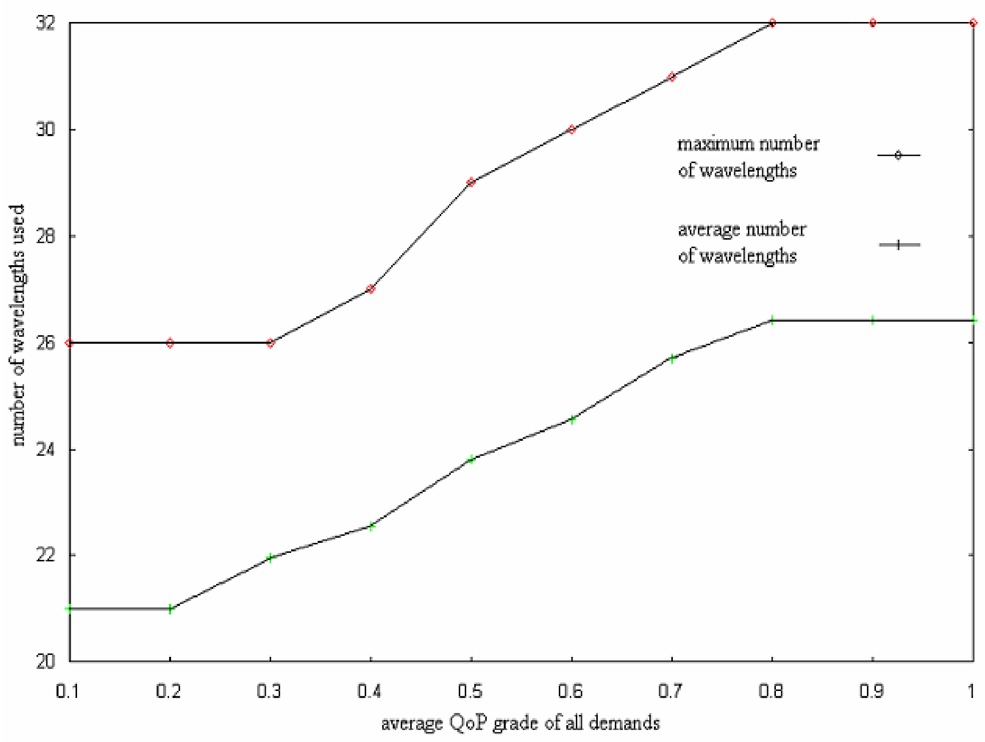


Figure 3.17 Wavelength Usage per Link in Modified 8-Node Network

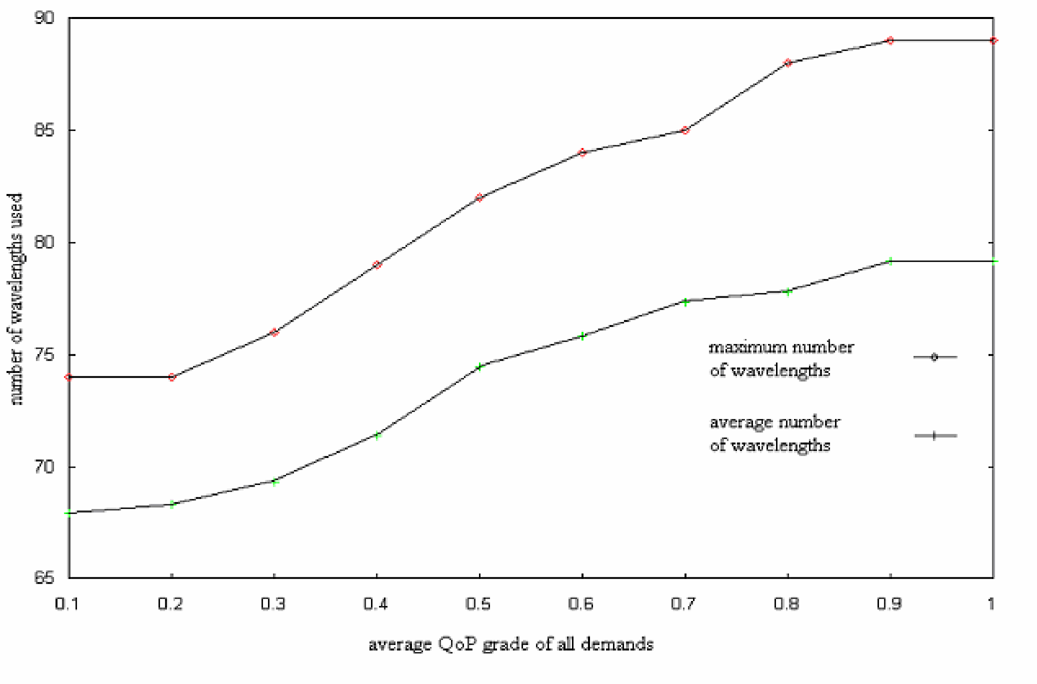


Figure 3.18 Wavelength Usage in Modified ARPANET

Due to the change in the network topologies, the average number of wavelengths per link is different compared with the original topology. More importantly, the load balancing results change significantly. In the 8-node network, even through only three links are removed, the maximum number of wavelengths used per link is increased significantly when compared with the increase in the average number of wavelengths. However in ARPANET, the load balancing results can be viewed as an acceptable one.

From the above comparison, we can conclude that the network connectivity is an important factor for load balancing. If the network connectivity is denser, load balancing can be done more effectively.

3.4 Simulation Results in Wavelength-limited Networks

The above simulation assumes that the wavelength per link is unlimited. When the number of wavelength in the network is limited, the provisioning problem's objective changes, i.e., maximize the total number of the acceptable connection requests.

This algorithm is similar to the one without wavelength limit. However, we do not provision the connection requests in fixed order as in the previous algorithm. It is based on the concept of wavelength layer. Let W represent the maximum number of wavelengths per link, and w represent current wavelength labeled from 1 to W in an ascending order. The algorithm is given bellow (refer to Figure 3.19).

1. Reserve one shortest path as backup path for each source-destination pair. Do not assign wavelengths for these backup paths, calculate the backup wavelength later.
2. Let $w = 0$.
3. Increase w by 1.
4. If $w > W$, i.e., no more wavelength available, go to step 9.
5. Update network topology by adding a new wavelength layer.
6. For any unaccepted connection request, say from s to d, route and assign wavelength for it, avoiding using the backup path with the same source and destination. Update the backup wavelength for the source-destination pair $s - d$ on the backup path.
7. Repeat step 6 for all the all unaccepted requests in this topology if possible.
8. If all connection requests are accepted, go to step 9. Otherwise, go to step 3.
9. Algorithm ends.

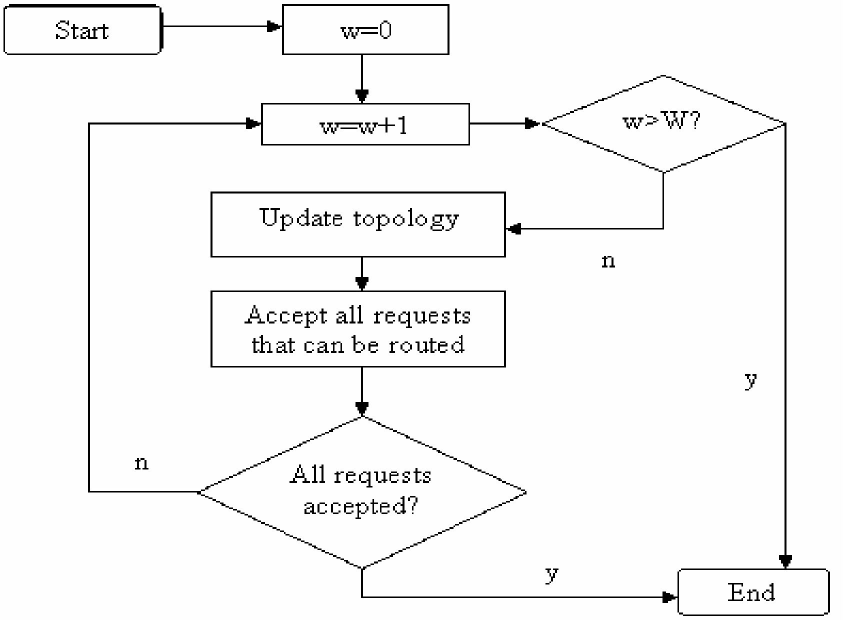


Figure 3.19 Algorithm for Wavelength Limited Networks

Without grouping the connection requests with the same source and destination, this algorithm is simpler compared with the previous one. For each w, i.e., at each wavelength layer, limited paths can be found because only one wavelength can be assigned for the paths at any link (i, j). Actually, the number of paths at any layer must be fewer than the number of links in the network, i.e., L, since a wavelength at any link can be used by at most one path. So the complexity of k-shortest paths searching at each layer is $O(N^2L)$. Since the wavelength limit in the network is W , the complexity of this algorithm is $O(N^2LW)$. The k-shortest paths searching plays the key role.

In this algorithm, to maximize the total number of acceptable connection requests, we loose some sharing efficiency, because we do not group the connection requests with the same source and destination. Under this situation, the backup path can not be fully utilized as in the scenario with grouping. In the simulation, we set the wavelength limit to 15 in the 8-node network, and 100 in ARPANET. The traffic increases step by step. The blocking probability in the two networks for various number of requests is shown in Figure 3.20 and Figure 3.21.

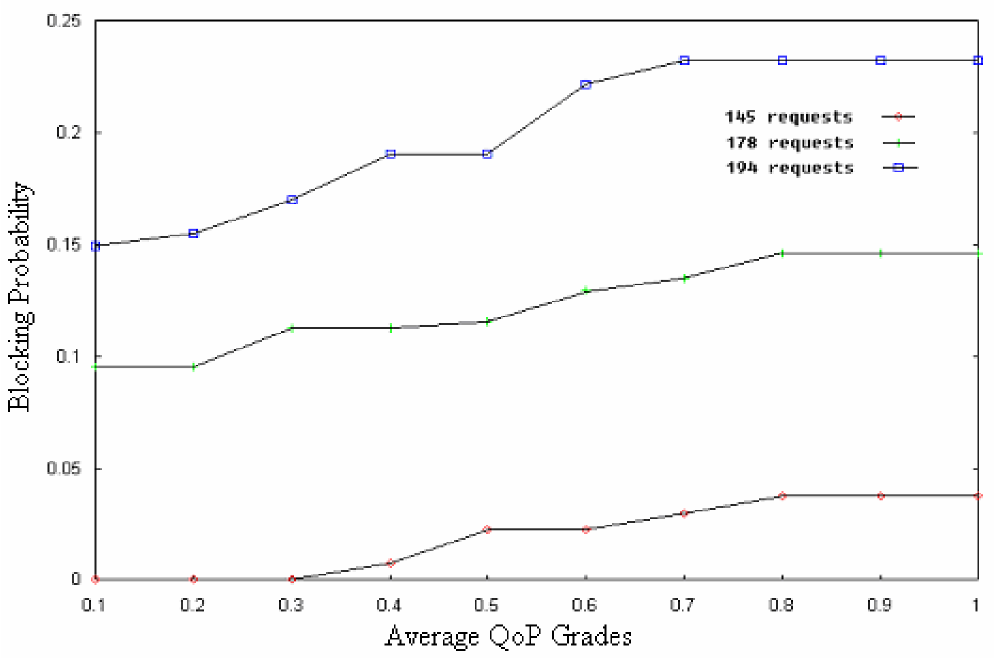


Figure 3.20 Blocking Probability in 8-Node Network with 15 Wavelengths per Link

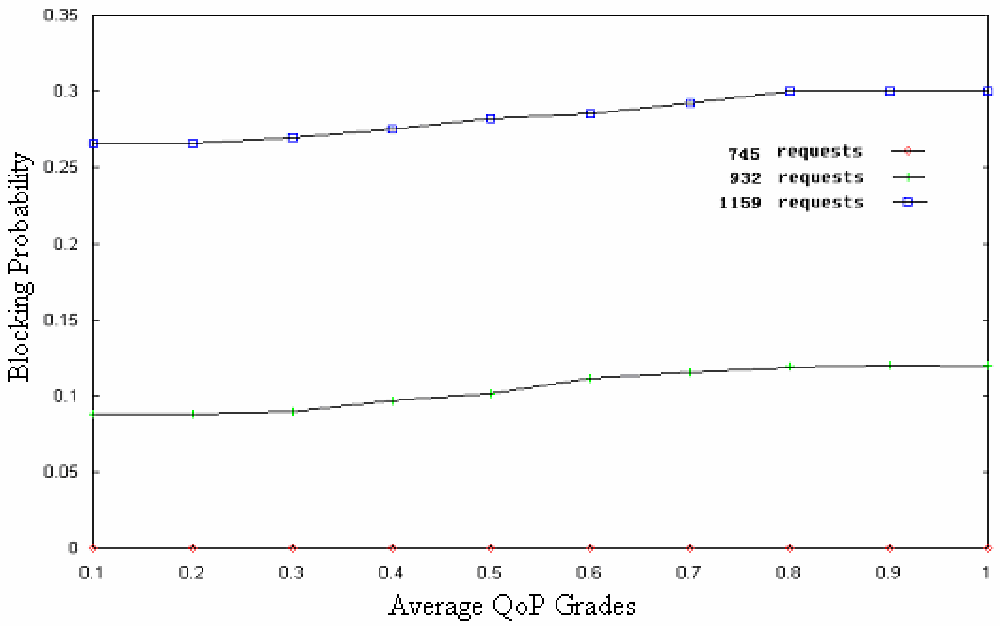


Figure 3.21 Blocking Probability in ARPANET with 100 Wavelengths per Link

As shown in the figures, the blocking probability increases as the traffic load becomes heavy and the average QoP grade grows. Since our algorithm routes the connection requests one by one, i.e., no grouping before routing, the bandwidth sharing of the backup paths among the same source-destination pair reduces. So the number of the connection requests affects the blocking probability more than the average QoP grade. As the average QoP grade increases, the total number of accepted connection requests does not change much, though the blocking probability is changing. The total number of acceptable connection requests in the 8-node network is about 152(± 8), while the total number of acceptable connection requests in ARPANET is about 830 (± 20).

Chapter 4: Provisioning in Networks without Wavelength Converters

In the previous chapter, we studied the performance of our algorithm in wavelength convertible networks. In wavelength convertible networks, wavelength converters are equipped at all the nodes in the network. Wavelength conversion eliminates the wavelength-continuity constraint in wavelength routed WDM networks. However, all-optical converters are very expensive. It is impractical to deploy full wavelength conversion capability at all nodes. Sparse Wavelength Conversion [39] may be a tradeoff between performance and the cost. To obtain good performance, only some of the nodes in the network need to be equipped with wavelength conversion capability. In this chapter, we provide an algorithm and simulation results for provisioning in a survivable WDM networks without wavelength convertibility.

4.1 Heuristic Solution for Non-Convertible Networks

optical networks can be viewed as a layered graph [3]. Any layer in this graph maps to a particular wavelength. In a wavelength-convertible network, nodes can be classified into two categories: wavelength-selective node and wavelength-converting node [3]. A node with wavelength convertibility is a wavelength-converting node. Otherwise, it is a wavelength-selective node.

In networks without wavelength convertibility, there is no wavelength converting node, such that the wavelength layers are disconnected with each other. Lightpaths can only be established within a single layer, i.e., any path in the network is a wavelength continuous path. To maximize the wavelength usage in the network, for each wavelength layer, any acceptable connection request should be routed and assigned the wavelength corresponding to this layer.

The following is the heuristic solution to the provisioning problem in a wavelength non-convertible network. The traffic model is the same as the one in wavelength convertible network.

1. Find a shortest path for each source-destination pair. These paths are reserved as the backup path for each $s-d$ pair. No wavelength assignment is done at this stage, because we do not know how many wavelengths are sufficient for the backup paths.
2. Let w represent the current wavelength number to be used for routing. Set w to 0.
3. $w = w + 1$, i.e., consider a new wavelength to all the links in the network. The w-th wavelength is said to be the current wavelength, and the wavelength layer associated to w is said to be the current wavelength layer.
4. Route the connection requests one by one in the current wavelength layer. For any connection requests with same source and destination nodes to be

routed in this layer, cut the links that the backup path for this connection request goes through before routing. This ensures the link disjointness between the primary paths and the backup paths. Update the network topology of this wavelength layer, and remove the links used by already-routed connection request before routing any other connection request. After this step, the current wavelength layer should be maximally utilized for the given connection requests and no unprocessed request can be allocated a route in this layer.

5. Check if all connection requests are routed and assigned wavelengths. If so, go to Step 6. Otherwise, go to Step 3.
6. For connection requests with same source and destination, check any links shared by the paths traversed by these requests. Calculate the backup bandwidth needed for these primary paths according to their QoP grades. Exchange the paths among the primary paths if it is necessary. Assign wavelengths for backup paths.

4.2 Simulation Results without Wavelength Limit

Figure 4.1 and Figure 4.2 show the total wavelength usage in the 8-node network and ARPANET.

4.2.1 Wavelength Usage

Figure 4.1 and Figure 4.2 show the total wavelength usage in the 8-node network and ARPANET.

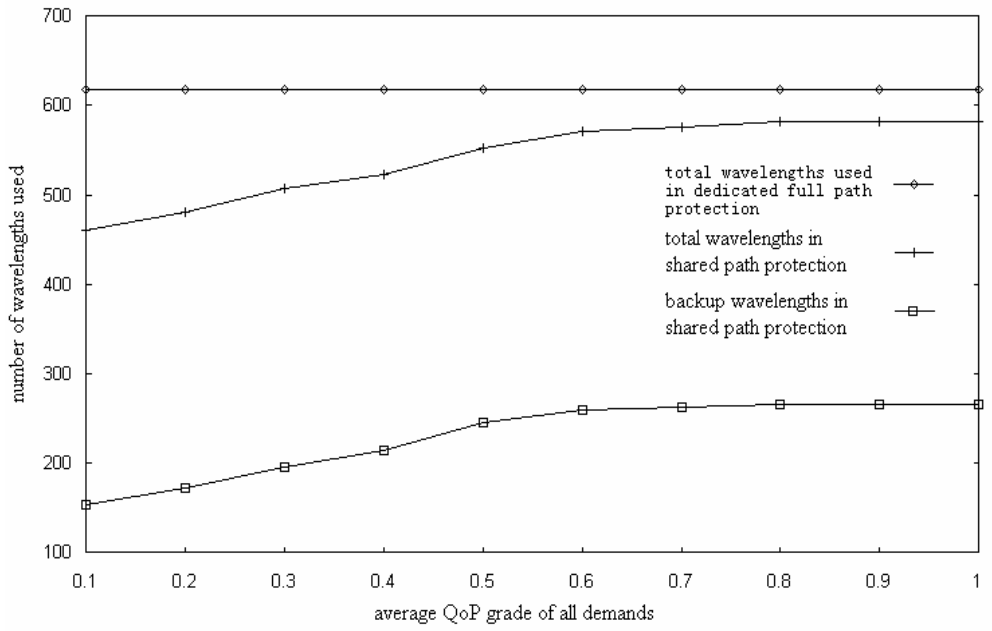


Figure 4.1 Wavelength Usage in the 8-Node Network

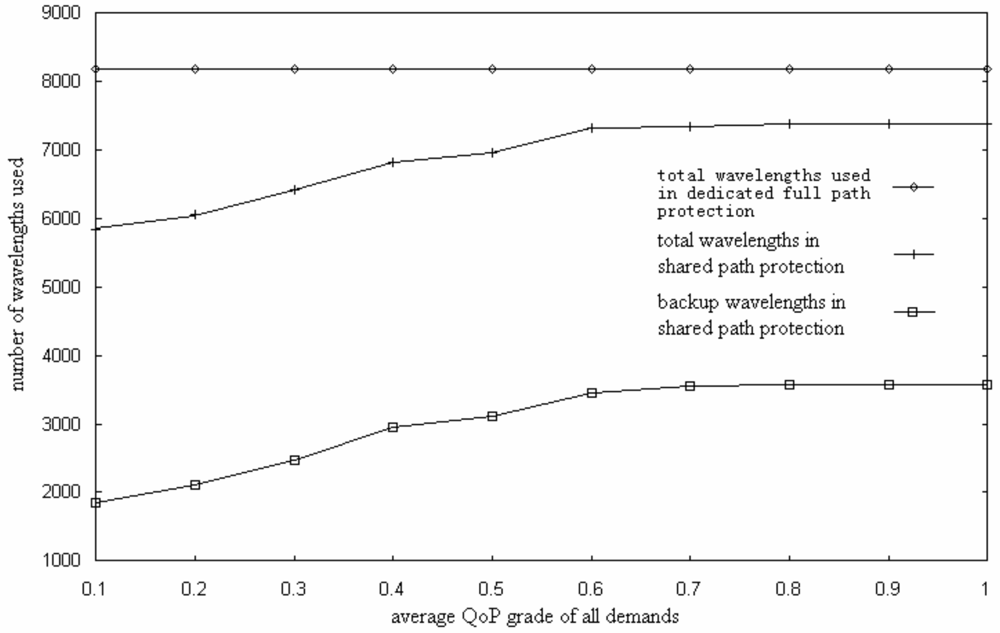


Figure 4.2 Wavelength Usage in ARPANET

As the QoP grade increases, the wavelength usage in both the two networks increases steadily. The trend is similar to the one in the wavelength convertible networks. We notice that the wavelength usage in a wavelength non-convertible network is slightly higher than the one in a wavelength convertible network with the same physical topology. This may be explained by the following example.

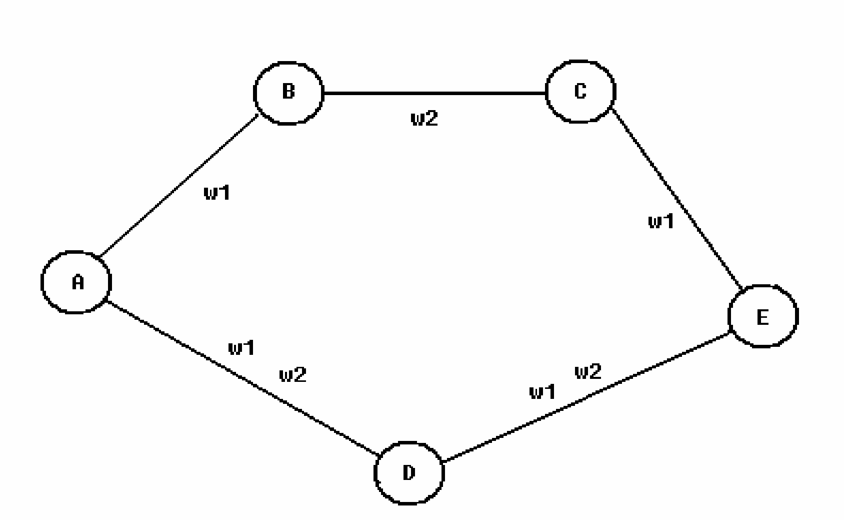
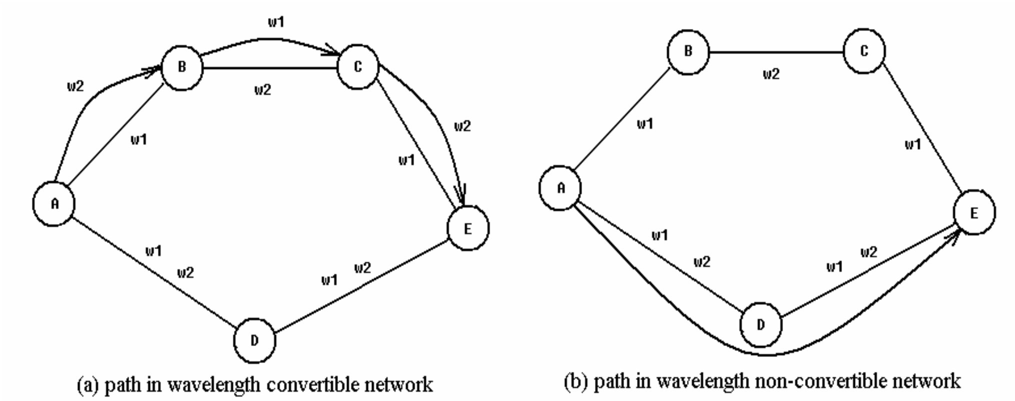


Figure 4.3 Network Topology and Wavelength Usage before Routing



(a) path in wavelength convertible network

(b) path in wavelength non-convertible network

Figure 4.4 Paths Found from A to E

Figure 4.3 shows the current physical network topology and the wavelength usage before route and wavelength assignment for a connection request from node A to node

E. On link (A, D) and link (D, E) wavelength $w1$ and $w2$ are used. On link (A, B) and (C, E) wavelength $w1$ is used, and on link (B, C) wavelength $w2$ is used. Assume that the bandwidth of this connection request is one wavelength. We choose the shortest path for the connection request. Figure 4.4 shows the paths found for this connection request. In wavelength convertible network (Figure 4.4.a), we choose the path A->B->C->E, though it is not the shortest one. Note that wavelength conversion should be done at node B and node C. In this case, three wavelengths are occupied. In wavelength non-convertible network, path A->B->C->E cannot be used due to the wavelength continuity constraint. Lightpath cannot be established if no wavelength is added to the network. Under the current state, one wavelength ($w3$ has to be added to this network to satisfy this connection request. After this wavelength is added, the shortest path A->D->E (Figure 4.4.b) is chosen for this connection request. In this example, a wavelength convertible network will consume three wavelengths to accept this connection request, while a wavelength non-convertible network consumes two wavelengths, it requires an additional wavelength to be added to the network.

From this example, we can see that in a wavelength convertible network, it is easier to find a path from source node to destination node without the help of additional wavelength. However, in a wavelength non-convertible network, when wavelength continuity constraint cannot be satisfied, new wavelength has to be deployed and a short path can be found after adding the new wavelength. Usually, if a wavelength continuous path can be used for a specific source-destination pair, this path can also be found in a network with wavelength convertibility, while the reverse case is not always true. Given a new wavelength in wavelength non-convertible network, the shortest path will be found, and the length of this path is not longer than the length of the path found in a wavelength convertible network. So the wavelength consumption in a wavelength convertible network is more than the one in wavelength non-convertible networks.

4.2.2 Load Balancing in Networks

Through the total wavelength consumed in a wavelength non-convertible network is slightly less than the one in a wavelength convertible network, it depends on the cost of the maximum number of wavelengths deployed in the network. Figure 4.5 and Figure 4.6 show the wavelength usage per link in the two networks.

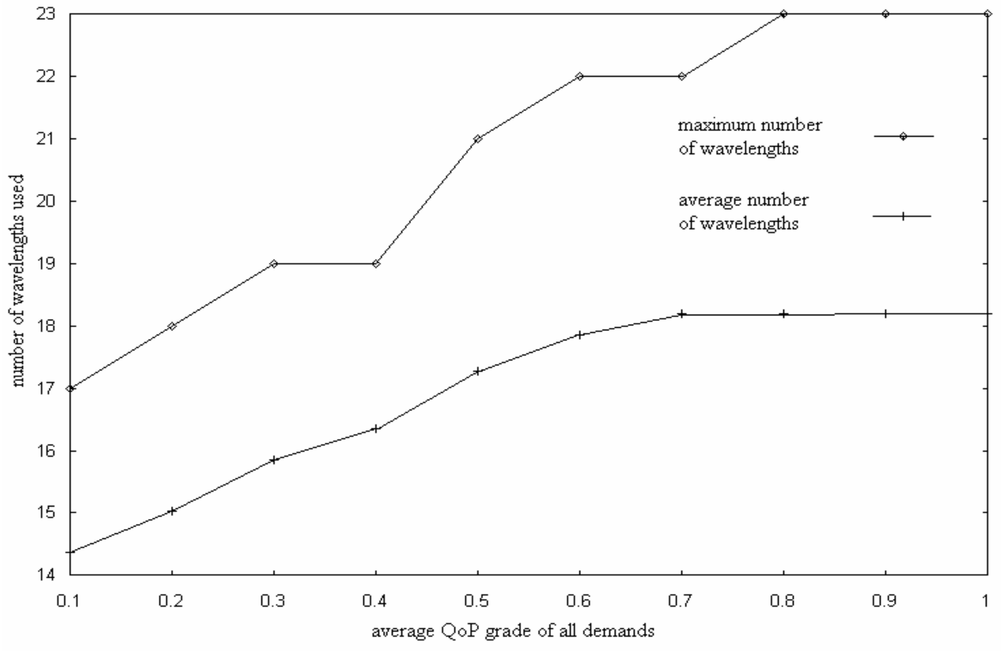


Figure 4.5 Wavelength Usage per Link in the 8-Node Network

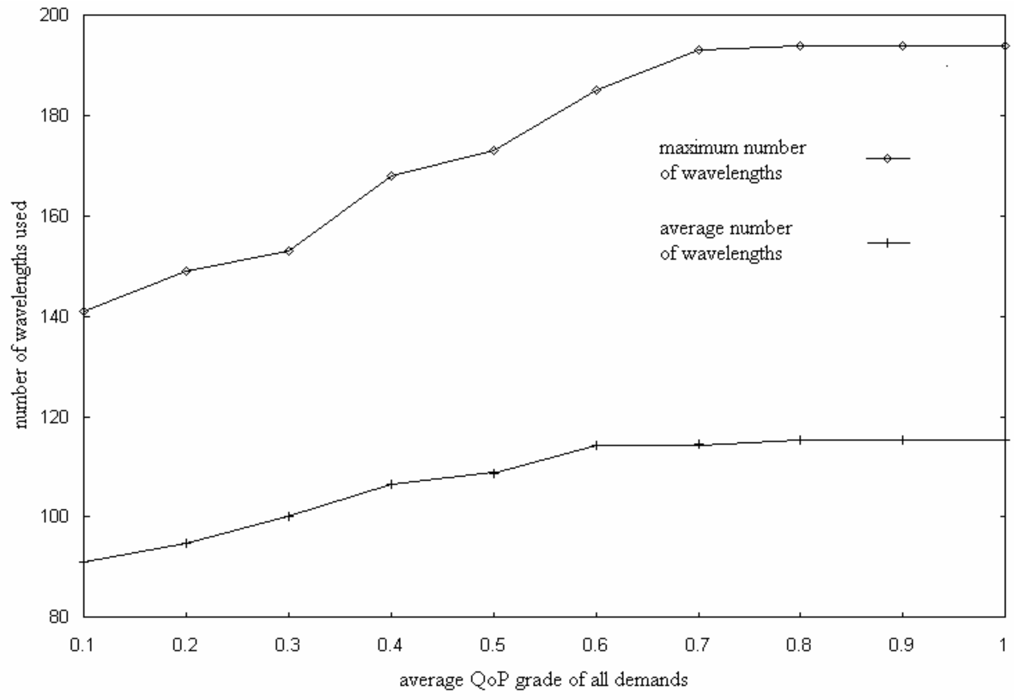


Figure 4.6 Wavelength Usage per Link in ARPANET

Compared to the results in wavelength convertible networks, the maximum number of wavelengths used in the wavelength non-convertible network is very large. In the 8-node simulation network, the largest difference occurs when the average QoP grade is above 0.7, where the maximum number of wavelengths used per link is 26.46% higher than the average one. The minimum difference occurs when the average QoP is 0.4, where the maximum number of wavelengths used is 16.28% higher than the average one per link. This result is similar to the one in the wavelength convertible ARPANET, in which the load balancing is not achieved well. The load balancing in wavelength non-convertible ARPANET is even worse. The maximum number of wavelengths is about 54.84% to 68.30% higher than the average one. This means that about 1/3 or more wavelengths in the network are idle after routing these connection requests.

4.3 Simulation Results in Wavelength-limited Networks

The solution for a network with wavelength limit is similar to the one in a wavelength convertible network as described in the previous chapter. It can be briefly described as follows.

1. Reserve one shortest path as backup path for each source-destination pair. Do not assign wavelengths for these backup paths, calculate the backup wavelength later.
2. Let w represent the current wavelength layer, and let $w = 0$.
3. Increase w by 1.
4. If $w > W$, i.e., no more wavelength available, go to step 9.
5. For any unaccepted connection request, say from s to d, cut the backup path for $s - d$ from the this layer (w-th layer) before routing. Route and assign wavelength for it. Update the backup wavelength for the source-destination pair $s - d$ on the backup path.
6. Repeat step 5 .
7. If all connection requests are accepted, go to step 8. Otherwise, go to step 3.
8. Algorithm ends.

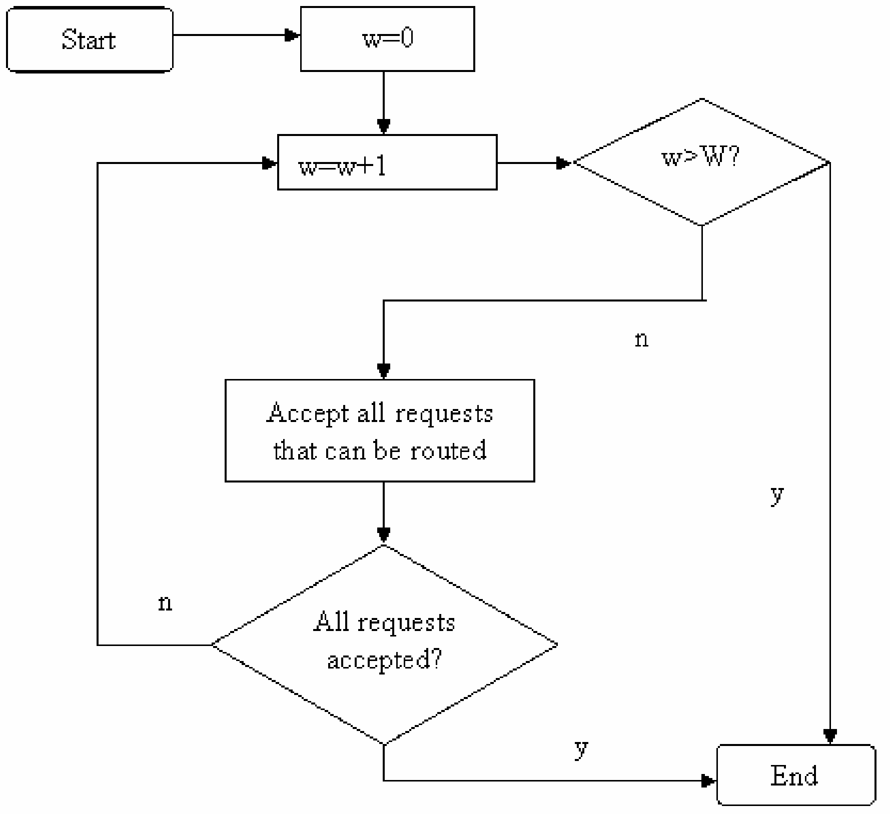


Figure 4.7 Algorithm for Wavelength Limited Network

Figure 4.7 shows the flowchart of this algorithm. The only difference is that there is no network topology update in this solution. In a wavelength convertible network, any free wavelength can be used later with the use of wavelength converters. However, in networks without wavelength converters, this wavelength cannot be used any more, because we have searched all the pending connection requests to accept them before adding a new wavelength to the network. Simulation results are shown in Figure 4.8 and Figure 4.9 for the two networks.

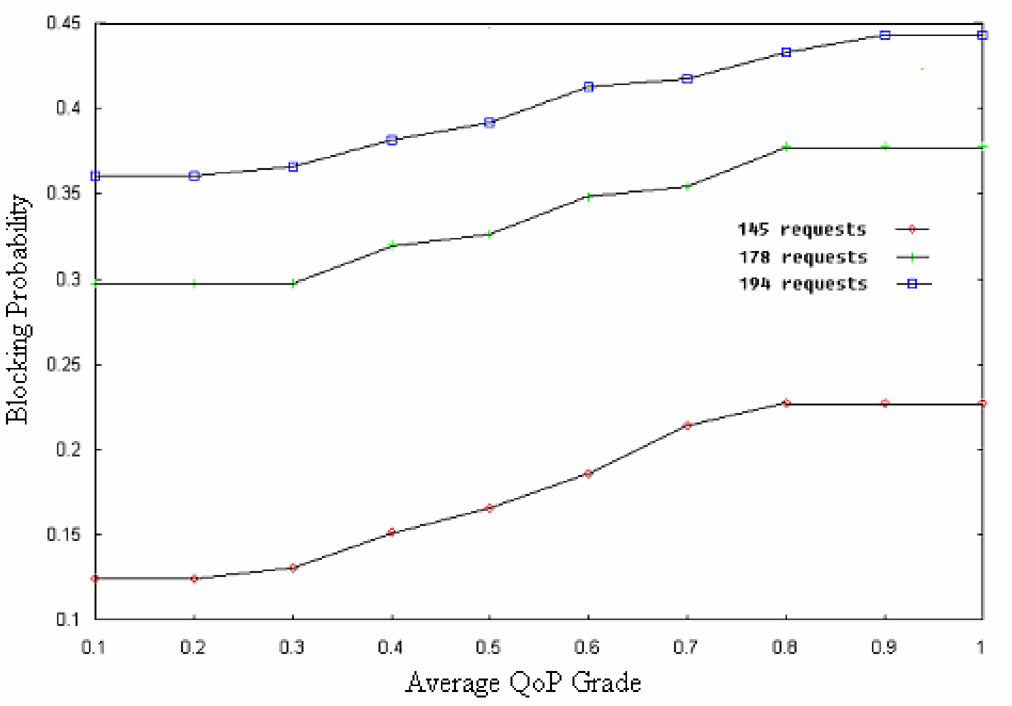


Figure 4.8 Blocking Probability in 8-Node Network with 15 Wavelengths per Link

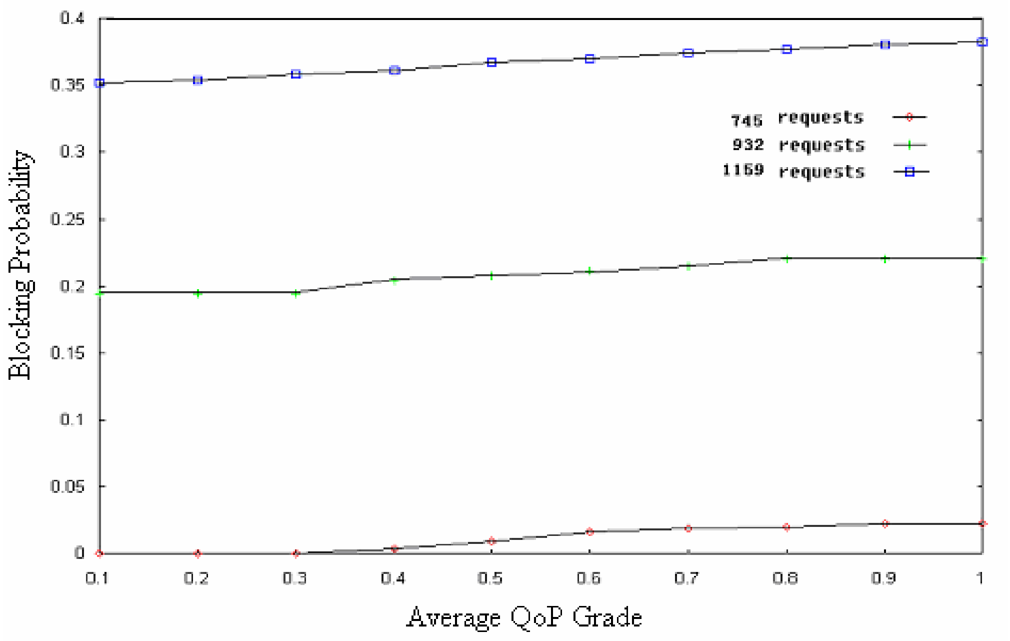


Figure 4.9 Blocking Probability in ARPANET with 100 Wavelengths per Link

These results are similar to those presented in Chapter 3. The number of connection requests still plays the key role in affecting the blocking probability. Due to the wavelength continuity constraint, the blocking probability is much higher than the one in wavelength convertible networks. At the same time, the network capacity is reduced. Without wavelength converter, the 8-node network can only handle about 116 (± 10), while the ARPANET can accept about 750 (± 20) requests.

Chapter 5: Conclusions and Future Work

The work presented in this thesis considers the provisioning problem in a survivable mesh network with QoP requirements. Problem formulation and heuristic algorithms were developed. Both the wavelength-convertible and wavelength non-convertible schemes were considered, and the case with wavelength limit in the network was also taken into consideration. To save network resources (wavelengths) in the network, quality of protection and shared path protection were used in our algorithm.

Simulations were conducted on two different network topologies. According to the simulation results, our algorithm performs well on a network with full wavelength convertibility, especially on a network with dense connectivity. The performance in networks without wavelength convertibility is poorer compared with networks with wavelength converters. In this case, both the number of un-utilized wavelengths and the blocking probability are higher than in networks with wavelength converters. This means that, in networks with wavelength convertibility, wavelength utilization efficiency is achieved at the cost of wavelength converters.

The algorithm for networks without wavelength convertibility does not perform as well as the one for networks with wavelength convertibility. Backup path sharing is not fully utilized in this case, because the connection requests are routed one by one even though they are from the same source to the same destination. Whereas, in the wavelength-convertible network, we can group these connection requests carefully to improve the sharing efficiency. How to improve further the efficiency of shared path protection in wavelength non-convertible networks is challenging for future work.

Furthermore, an extensive study can be conducted in a network with sparse wavelength conversion. Networks with wavelength convertibility and without convertibility are the ideal and worst state for provisioning, and we presented our solutions and simulation results for these two extreme situations. Networks with sparse wavelength convertibility are also becoming practical in a real networking environment. They provide attractive tradeoffs between the consumptions of wavelengths and converters. Determining the sufficient and necessary bandwidth in this scenario is a future challenge.

In out work, we considered static traffic demands with quality of protection requirements in arbitrary mesh networks. A possible future work is to study the dynamic traffic demand with quality of protection requirements and compare how well they perform when compares to other traditional approaches.

References

[1] William Stallings, “High-Speed Networks and Internets:

Performance and Quality of Service”, 2nd Edition, Prentice Hall, 2002.

[2] Steven Shepard, "SONET/SDH Demystified", New York: McGraw-Hill, 2001.

[3] C. Siva Ram Murthy and Mohan Gurusamy, “WDM Optical Networks: concepts, design, and algorithms”, Prentice Hall, 2002.

[4] Sudhir S. Dixit, “IP OVER WDM: Building the Next Generation Optical Internet”, John Wiley & Sons, Inc., 2003.

[5] S. Shenker, C. Partridge, and R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997.

[6] Geoff Huston, “Internet Performance Survival Guide: QoS strategies for multi-service networks”, New York : J. Wiley, 2000.

[7] P. Veitch, I. Hawker, and G. Smith, “Administration of Restorable Virtual Path Mesh Networks”, IEEE Communications Magazine, Vol. 34, No. 12, pp. 96-102, December 1996.

[8] I. Chlamtac, A. Ganz, and G. Karmi, “Lightnet: lightpath based solutions for wide bandwidth WANs”, INCOM’90, Vol. 3, pp. 1014-1021, 1990.

[9] O. Gerstel and G. Sasaki, “Quality of Protection (QoP): a quantitative unifying paradigm to protection service grades”, Optical Networks Magazine May/June 2002.

[10] J. Y. Wei, et al., “Network Control and Management for the Next Generation Internet”, IEICE Trans. On Communications, Vol.E83-B, No.10, October 2000, pp.

2191-2209.

[11] Stamatios V. Kartalopoulos. “Introduction to DWDM Technology”, New York: IEEE Press, 2000.

[12] Uyless Black, “MPLS and Label Switching Networks”, Upper Saddle River, NJ : Prentice Hall PTR, c2002.

[13] Sean Harnedy, “The MPLS Primer: an introduction to Multiprotocol Label Switching”, Upper Saddle River, NJ : Prentice Hall PTR, 2002.

[14] G. K. Chang, et al., “A Proof-of-Concept, Ultra-low Latency Optical Label Switching Tested Demonstration for Next Generation Internet Networks”, OFC’2000, Vol.2, Section WD5, pp.56-58, Baltimore, Maryland, March 2000.

[15] J. Y. Wei and R.I. McFarland Jr, “Just-in-time Signaling for WDM Optical Burst Switching Networks”, IEEE Journal of Lightwave Technology, Vol.18, No.12, December 2000.

[16] Y. Xiong, M. Vanderhoute, and CC Cankaya, “Control Architecture in Optical Burst-Switched WDM Networks”, IEEE Journal on Selected Areas in Communications, Vol.18, No.10, October 2000.

[17] Z. Zhang, et al., “Lightpath Routing for Intelligent Optical Networks”, IEEE Network, July/August 2001.

[18] D. Benjamin, et al., “Optical Services over the Intelligent Optical Network”, IEEE Communications Magazine, September 2001.

[19] S. D. Maesschalck, et al., “Intelligent Optical Networking for Multilayer Survivability”, IEEE Communications Magazine, January 2002.

[20] John Strand, Angela Chiu and Robert Tkach, "Issues for Routing in the Optical Layer", IEEE Communication Magazine, pp.81-87, February 2001.

[21] L. Sahasrabuddhe, S. Ramamurthy, and B. Mukherjee, "Fault Management in IP over WDM Networks: WDM protection versus IP protection", IEEE Journal on Selected Areas in Communications, Vol. 20, No. 1, pp. 21-33, January 2002.

[22] J. Y. Wei, et al., "Connection Management for Multiwavelength Optical Networking", Journal on Selected Areas in Communications, Vol.16, No.7, pp.1097, July 1998.

[23] Vishal Sharma, et al., "Framework for MPLS Based Recovery", IETF Internet Draft.

http://www.ietf.org/proceedings/01aug/I-D/draft-ietf-mpls-recovery-frmwrk-03.txt, July 2001.

[24] Riza Cetin, et al., "Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute", IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-mpls-fastreroute-mib-01.txt, November 2002.

[25] Black, Uyless D, "MPLS and Label Switching Networks", Upper Saddle River, NJ : Prentice Hall, 2001.

[26] J.Moy, OSPF Version 2. IETF RFC 2328, April 1998.

[27] C.Villamizar. OSPF-OMP, IETF draft 1998.

[28] Rajiv Ramaswami and Kumar N. Sivarajan, "Optical Networks: A Practical Perspective", Second Edition, Morgan Kaufmann Publishers, October 2001.

[29] Murat Alanyali and Ender Ayanoglu, “Provisioning Algorithms for WDM Optical Networks”, IEEE/ACM Transactions on Networking, Vol. 7., No.5, October, pp767-778, 1999.

[30] A. Shami, Chadi Assi, and Mohammed Ali, “Dynamic Wavelength Provisioning in DWDM-Based Optical Network”, IFIP TC6 Fifth Working Conference on Optical Network Design and Modelling (ONDM 2001), pp. 357-370, February 5-7, 2001.

[31] A. E. Ozdagla and D. P. Bertsekas, “Routing and Wavelength Assignment in Optical Networks”, IEEE/ACM Transactions on Networking, Vol. 11, No.2, pp.259-272, April 2003.

[32] A. Mokhtar and M. Azizoglu, “Adaptive Wavelength Routing in All Optical Networks”, IEEE/ACM Trans. Net, Vol.6, pp.197-206, April 1998.

[33] D. Banerjee and B. Mukherjee, “A Practical Approach to Routing and Wavelength Assignment in Large WDM Routed Networks”, IEEE Journal on Selected Areas in Communications, Vol.14, pp.903-908, June 1996.

[34] Martin Heusse and Yvon Kermarrec, “A New Routing Policy for Load Balancing in Communication Networks”, ACS/IEEE International Conference on Computer Systems and Applications 2001: 267-272.

[35] I. Matta and A.U. Shankar, “Type-of-Service Routing in Datagram Delivery Systems”, IEEE Journal on Selected Areas in Communications, vol.13, No.8, pp.1411-1425, October 1995.

[36] P. Veitch, I. Hawker, and G. Smith, “Administration of Restorable Virtual Path Mesh Networks”, IEEE Communications Magazine, vol. 34, No. 12, pp.96-102,

December, 1996.

[37] Thompson, Gerald E, “Linear Programming; an elementary introduction”, New York , Macmillan, 1971.

[38] R. Bhandari, “Survivable Networks, Algorithms for Diverse Routing”, Kluwer Academic Publishers, 1999.

[39] S. Subramaniam, M. Azizoglu, and A. Somani, “All-Optical Networks with Sparse Wavelength Conversion”, IEEE/ACM Transactions on Networking, Vol.4, No.4, pp. 544-557, August 1996.