**Master's Thesis**

Title

# Design Method for Logical Topologies with Quality of Reliability in WDM Networks

Supervisor

Professor Masayuki Murata

Author

Junichi Katou

February 13th, 2002

Department of Informatics and Mathematical Science

Graduate School of Engineering Science

Osaka University

Master's Thesis

Design Method for Logical Topologies with Quality of Reliability in WDM Networks

Junichi Katou

## Abstract

According to a rapid growth of the bandwidth capacity of the WDM network, traffic loss due to a failure of the network components is becoming unacceptable. To overcome this problem, a protection method that prepares backup lightpaths for each working path is now considered to enhance the reliability of networks. In this thesis, we first introduce a new concept of QoR (Quality of Reliability), which is one realization of QoS with respect to the reliability suitable to the WDM network. We define QoR in terms of a recovery time from when a failure occurs to when traffic on the affected primary lightpath is switched to the backup lightpath. We then propose a heuristic algorithm to design a logical topology with satisfying QoR requirement for every node pair. Our objective is to minimize the number of necessary wavelengths on a fiber in the logical topology to carry the traffic with required QoR. We compare our newly proposed algorithm with existing two algorithms and show that our proposed algorithm can utilize wavelength resources effectively; by using our proposed algorithm, the number of necessary wavelengths is at most 25% less than those by the other two algorithms.

## Keywords

WDM network, protection method, logical topology design algorithm, QoR (Quality of Reliability), layered graph

# Contents

# List of Figures

# List of Tables

# 1 Introduction

WDM (Wavelength Division Multiplexing) has a capability of providing a large transmission capacity by multiplexing wavelengths on the fiber. Recently, an IP (Internet Protocol) over WDM network where IP packets are directly carried over the WDM network is expected to offer an infrastructure for the next generation Internet. A currently available product for IP over WDM networks only provides the large bandwidth on the point–to–point link (Figure 1). That is, each wavelength on the fiber is treated as a physical link between the conventional IP routers. In this way, the link capacity is certainly increased by the number of wavelengths multiplexed on the fiber, but it is insufficient to resolve the network bottleneck against an explosion of traffic demands since it only results in that the bottleneck is shifted to an electronic router.

One promising way to alleviate the bottleneck is to configure wavelength paths over the WDM physical network and to carry IP packets utilizing the wavelength paths. Here, the physical network means an actual network consisting of the optical nodes and optical–

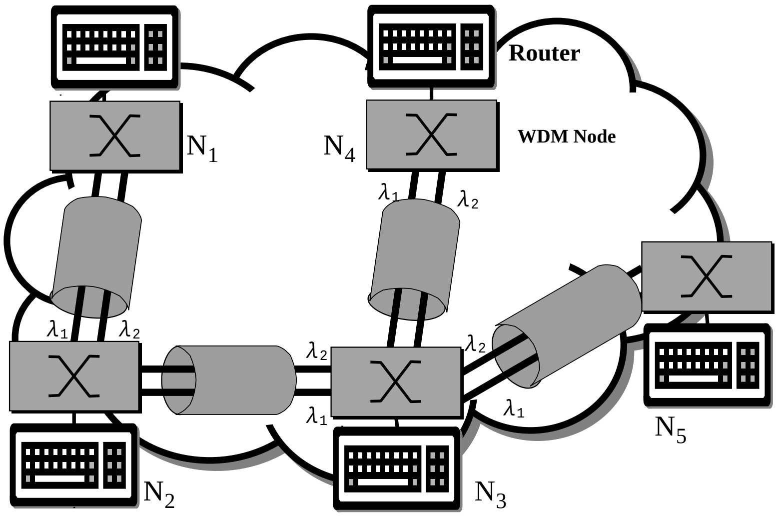


Figure 1: WDM Link Network

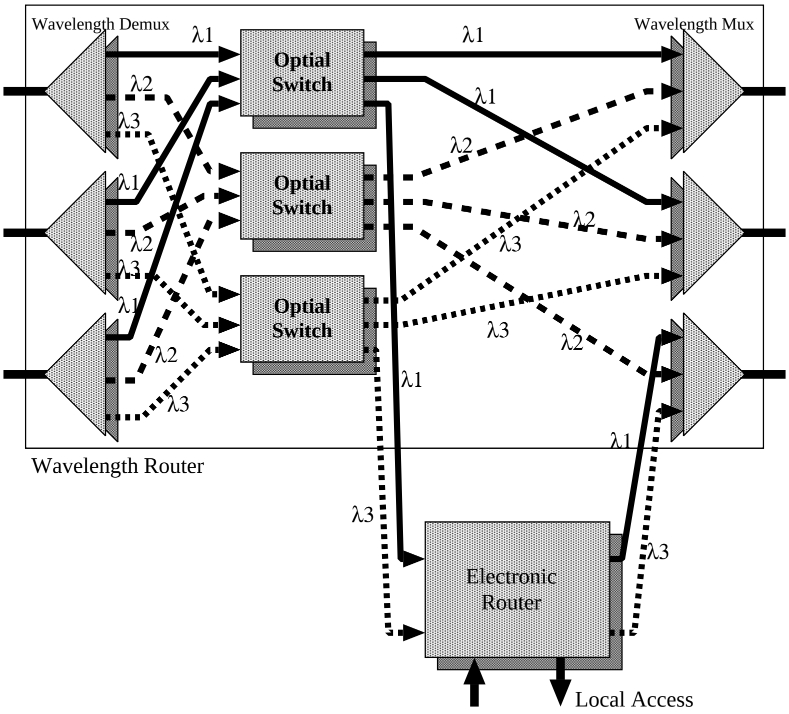


Figure 2: Optical Node Architecture

fiber links connecting two nodes. Each node in the wavelength–path network has optical switches directly connecting an input wavelength to an output wavelength, by which no electronic processing is necessary at the node (Figure 2). The incoming multiplexed signals are divided into each wavelength at the wavelength demux. Then, each signal is routed to an optical switch. The optical switch switches incoming signals to a preconfigured outgoing port. Finally, signals routed to wavelength mux are again multiplexed and transmitted to the next node. Then, the wavelength path can be set up directly between two nodes via one or more optical switches. Hereafter, we will call the wavelength path directly connecting two nodes as a *lightpath* (Figure 3). Viewing from the upper layer than the optical layer (e.g., IP layer), the nodes are directly connected via the lightpath. Utilizing lightpaths, another topology is embedded over the physical topology (Figure 4), and it is called the *logical topology*.

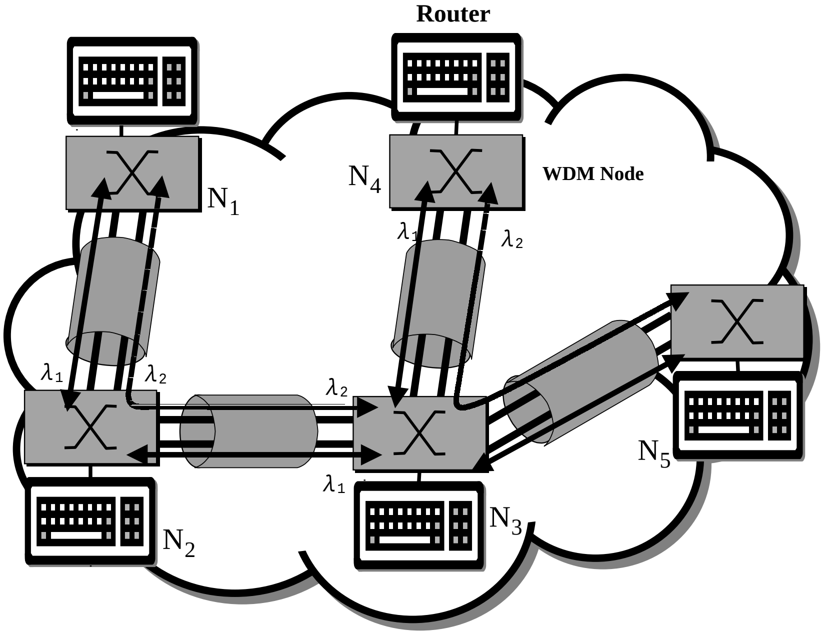


Figure 3: WDM Path Network

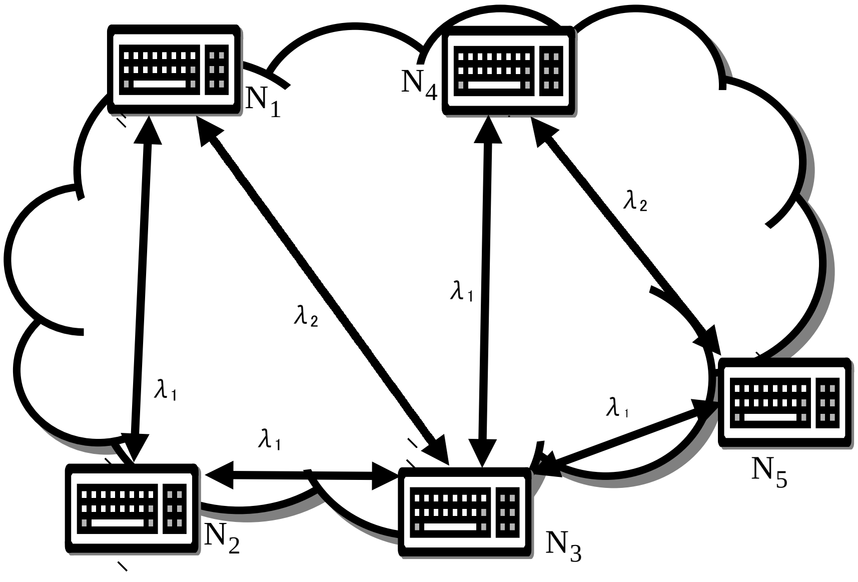


Figure 4: Logical Topology viewed by the IP Layer

According to a large transmission capacity of the WDM network, traffic loss due to a failure of network components is also becoming large. To overcome this problem, a *protection method* and a *restoration method* are now considered [1, 3-7]. Protection is a method to provide a fast recovery by switching the working lightpaths affected by the failure (hereafter we call the working lightpath as a *primary lightpath*) to backup lightpaths, each of which is prepared for the primary lightpath before a failure occurs [3]. By preparing backup lightpaths properly, the protection method can guarantee 100% recovery from the failure if it is assumed that more than two components never fail at the same time (i.e., the single–failure assumption). On the contrary, the restoration method tries to dynamically discover the route and wavelength of backup lightpaths after the failure occurs [3]. Therefore, the restoration method may fail the failure recovery if the unused wavelengths are not available. Moreover, the restoration method tends to require more time to recover from the failure than the protection method, because the restoration method requires the time for finding backup lightpaths by signaling.

Determining the route and wavelength of primary/backup lightpaths is called a logical topology design method [1, 8, 9]. Most of conventional methods for designing the logical topology with protection/restoration methods focuses on minimizing the number of wavelengths used in the WDM network [3-5], or minimizing the blocking probability to set up lightpaths [6, 7]. Note that the blocking probability is the probability that lightpath set up request is rejected due to a lack of the available lightpaths. Reference [1] proposes to reduce the number of necessary wavelengths by allowing that the backup lightpaths, whose routes are disjoint with each other, can share the same wavelength resources by assuming a single failure. More recent researches focus on providing QoS (Quality of Service) with respect to a failure recovery in the optical WDM network [4, 5]. QoP (Quality of Protection) is then introduced to realize QoS in the optical network [4]. The authors in [4] propose a probabilistic failure recovery model where only the fraction of traffic, which can be specified by the user, is recovered from the failure. Unlike the approaches in [1, 4, 7], reference [5] considers the situation that more than two components may fail at same time (a multiple–failure assumption). Reference [5] then assumes that each primary lightpath has its own reliability metric, which is determined from failure probabilities of network components. Then, backup lightpaths are partially configured for the primary lightpath so as to satisfy the specified probability. However, in those QoP–based lightpath configuration methods, the quality for the failure recovery is guaranteed only in a probabilistic manner. That is, the above researches tries to improve the effective usage of network resources at the sacrifice of 100% guarantees of the failure recovery.

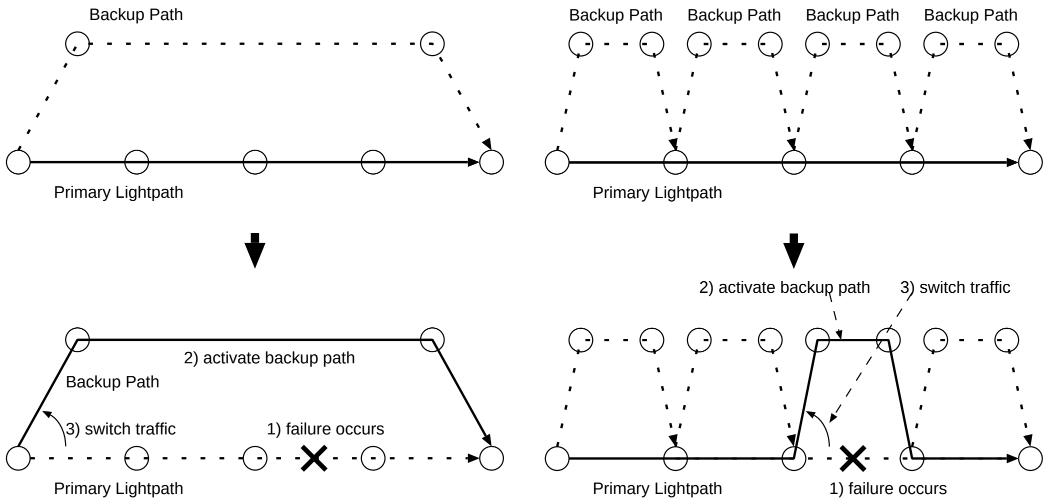
In this thesis, on the contrary, we introduce QoR (Quality of Reliability) as a new QoS metric that provides highly reliable lightpaths. In our QoR, the time to recover from the single failure is guaranteed as well as the 100% failure recovery, with a projection that building a highly reliable network becomes more important than utilizing the resources efficiently, especially as the number of wavelengths are increased by the recent advancement of the WDM technology. In other words, our approach is that we build a logical topology by utilizing wavelengths in an effective manner in order to guarantee the failure recovery time as well as to guarantee the 100% failure recovery. In [10], we proposed two heuristic algorithms to design the logical topology while satisfying QoR requirements of each connection. In this thesis, we will propose a new effective method, and compare our proposed algorithms in terms of the number of wavelengths needed to build the logical topology with QoR requirements.

This thesis is organized as follows. We show a brief introduction to the protection/restoration methods and introduce conventional researches with respect to the quality metrics for fault tolerance functionality. In Section 3, we introduce our proposed QoR (Quality of Reliability), and also describe a method to satisfy QoR in Section 4. We also propose a heulistic algorithm to design the logical topology satisfying QoR requirements in Section 4. In Section 5, we will compare and evaluate our proposed algorithms. Finally, Section 6 concludes this thesis.

# 2 Fault Tolerance Methods in WDM Networks

## 2.1 Protection Method [1, 2]

The protection method is the fast recovery method realized by mechanical switching in an optical domain. For each primary lightpath, backup lightpaths are determined beforehand and statically configured, and wavelengths for the backup lightpaths are reserved. There are two protection methods; path protection and link protection. In the path protection, backup lightpath is prepared between the source node and destination node (Figure 5(a)). On the contrary, in the link protection, backup lightpaths are prepared for each link of the primary lightpath (Figure 5(b)). In either case, when a failure occurs at some network component along the primary lightpath, the corresponding backup lightpath is activated and traffic on the primary lightpath is switched to the backup lightpath. By using the protection method, primary lightpaths are guaranteed the 100% reliability under the single–failure assumption. That is, whatever the failure occurs, the lightpath can be



(a) Path Protection (b) Link Protection

Figure 5: Protection Method

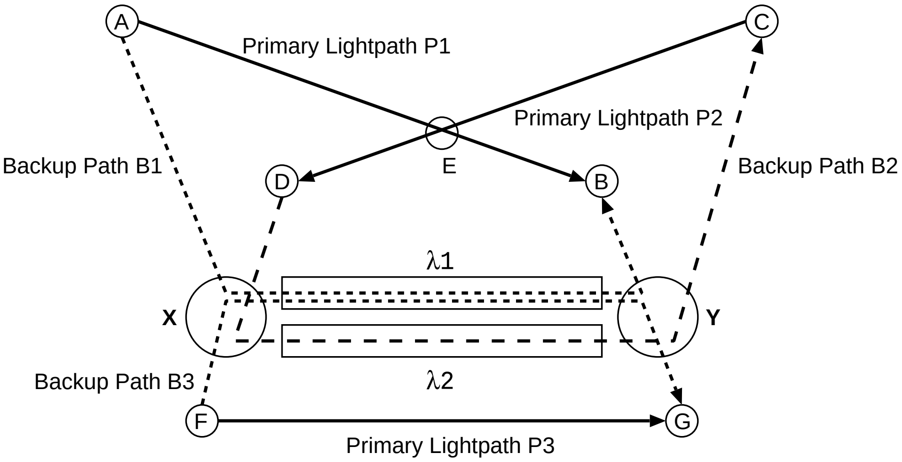


Figure 6: Shared Protection Method

recovered form the failure and the bandwidth for the lightpath never be reduced even after the failure. However, since the protection method reserves wavelengths for backup lightpaths, the effectiveness of wavelength usage decreases, and there is a trade–off relationship between the fast recovery and an effective usage of wavelength resources.

Accordingly, several methods have been proposed to use wavelengths effectively [1, 3-7]. One of the promising methods is *shared protection* where two or more primary lightpaths share the same backup lightpath as far as the primary lightpaths are disjoint [1]. Figure 6 illustrates the idea of shared protection. In Figure 6, three primary lightpaths (denoted as $P1$, $P2$ and $P3$) are shown. $P1$ is placed between nodes $A$ and $B$, and $P2$ and $P3$ are placed between nodes $CD$ and $FD$, respectively. Backup lightpaths $B1, B2$, and $B3$ protect the primary lightpaths $P1$, $P2$, and $P3$, respectively. The primary lightpaths, $P1$ and $P2$, traverse the same node $E$ as an intermediate node. Further, the backup lightpaths, $B1$, $B2$, and $B3$, are configured to use the link between node $XY$ in the current example. Here, $B1$ and $B3$ share the same wavelength $\lambda1$, whereas $B2$ uses $\lambda2$. Note that $B1$ and $B2$ must use different wavelengths on the link since the corresponding primary lightpaths ($P1$ and $P2$) utilize the same node $E$. If it is assumed that two or more components may fail at the same time, we cannot employ the shared protection method. This is because the shared protection method assumes that backup lightpaths, whose primary lightpaths are disjoint, never be activated at the same time, and hence the shared wavelength on the link is never conflicted by sharing backup lightpaths.

## 2.2 Restoration Method

A restoration method is an alternative to recover from failures at the optical layer. In the restoration method a backup lightpath is dynamically determined when a failure occurs. Once the backup lightpath is found, the traffic on the primary lightpath affected by the failure is switched to the backup lightpath. Unlike the protection method, the restoration method does not consume any wavelength resources for backup lightpaths before the failure. Therefore, an effective usage of wavelengths can be expected compared to the protection method. However, the restoration method may fail setting up the backup lightpath when available wavelength resources are not found. It means that the restoration method cannot guarantee the 100% failure recovery of lightpaths. Moreover, in the restoration method, since the backup lightpath is determined after the failure occurs, it takes an additional time to recover the lightpaths from the failure.

## 2.3 Quality Metrics in Existing Fault Tolerance Methods

Many researches have discussed the methods to design logical topologies with protection [1, 4, 5]. Most of existing protection methods try to minimize the number of wavelengths in designing the logical topology or maximize the total throughput within the network. The shared protection method is one of the effective methods to further reduce the number of necessary wavelengths by virtue of the single–failure assumption.

Recently, reference [4] propose to utilize the wavelength resources more effectively by introducing several guarantee classes with respect to the probabilities of the failure recovery. Note that the conventional protection method only guarantees the complete failure recovery (i.e., a single class of 100% guarantee). In [5], the authors introduce another guarantee class receiving a smaller probability of the failure recovery. That is, connections with requesting the higher class are provided backup lightpaths with the larger the probability of the failure recovery.

In this thesis, we introduce a new metric in order to define QoS with respect to reliability provided by the optical layer. It is a maximum recovery time, which is the maximum time between the time when a failure occurs and the time when the traffic is switched to the backup lightpath. We call this new metric as QoR (Quality of Reliability), and we want to guarantee the maximum recovery time according to the request by users, in addition to the 100% existence of the backup lightpath.

# 3 QoR (Quality of Reliability) and Recovery Time Modeling

## 3.1 QoS Classification based on Maximum Failure Recovery Time

In our QoR definition, the class is associated with the maximum recovery time. By specifying its QoR class, each connection is guaranteed its corresponding maximum recovery time upon a failure. In our proposed QoR, $QoR_1$ (the highest class) is guaranteed the minimum time of the failure recovery. $QoR_\infty$ is provided no protection lightpath, and the actual failure recovery may be left to the upper layer protocol (e.g., IP). More specifically, $QoR_n$ is guaranteed the maximum recovery time associated with class $n$, denoted as $RT(QoR_n)$. One of its simplest forms is

$$RT(QoR_n) = a + b * f(n), \tag{1}$$

where $a$, $b$ and $f(n)$ is determined by the network administrator based on the network environment. By configuring $f(n)$, QoR class can be represented in an arithmetic, geometric progression, or any other form. In numerical evaluation of Section 5, we will simply set $f(n)$ as

$$f(n) = n - 1 \tag{2}$$

and $a = D_{min}$ as the minimum recovery time, which includes a time to switch from the primary lightpath to the backup lightpath. $b = D_{scale}$ is the step–width of the recovery time, which includes the processing time to propagate the failure information and to reserve wavelengths at each node of the backup lightpath. The functions $RT(QoR_n)$ should be determined properly according to a given network environment, however, specification of only a class–dependent recovery time is not sufficient and it is possible to consider a more precise form of the recovery time. We discuss the node–pair dependent recovery time next.

Table 1: QoR (Quality of Reliability)

| | |
|---|---|
| $\text{QoR}_1$ | failure recovery within $D_{min}$ |
| $\text{QoR}_2$ | failure recovery within $(D_{min} + D_{scale})$ |
| $\text{QoR}_3$ | failure recovery within $(D_{min} + 2D_{scale})$ |
| $\vdots$ | $\vdots$ |
| $\text{QoR}_n$ | failure recovery within $(D_{min} + (n-1)D_{scale})$ |
| $\vdots$ | $\vdots$ |
| $\text{QoR}_\infty$ | no protection lightpath provided |

### 3.2 QoR Specification for Each Node Pair

There may be no route to configure backup lightpaths to guarantee the maximum recovery time defined in the QoR class. Figure 7 shows such an example. In Figure 7, there are two routes from node $A$ to $F$. The one is $[A \rightarrow B \rightarrow C \rightarrow D \rightarrow E \rightarrow F]$ and the other is $[A \rightarrow G \rightarrow H \rightarrow F]$. The propagation delay of the first route is 25ms in total while the second route is 44ms. In this situation, if node pair $AF$ requires a QoR class with

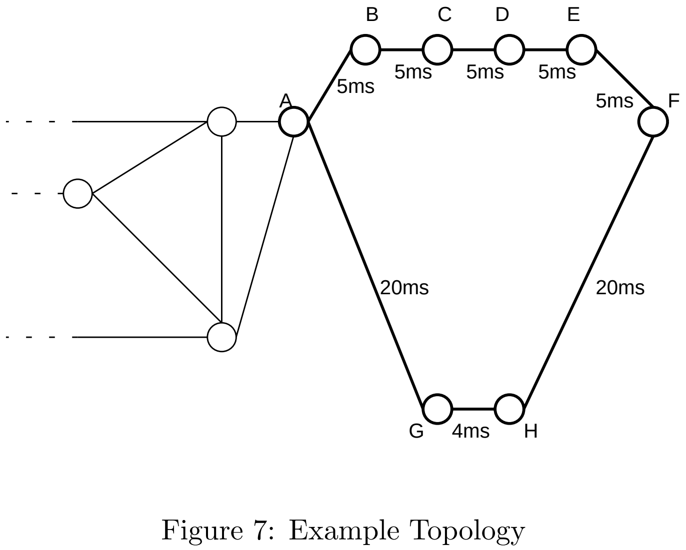


Figure 7: Example Topology

Table 2: QoR dependent on Node Pair

| QoR | Maximum Recovery Time | $QoR_{12}$ |  | $QoR_{ij}$ |  |
|---|---|---|---|---|---|
| $QoR_1$ | $D_{min}$ | — |  | — |  |
| $QoR_2$ | $D_{min} + 1 * D_{scale}$ | — |  | $QoR_{ij}(1)$ |  |
| $QoR_3$ | $D_{min} + 2 * D_{scale}$ | $QoR_{12}(1)$ | $\cdots$ | $QoR_{ij}(2)$ | $\cdots$ |
| $QoR_4$ | $D_{min} + 3 * D_{scale}$ | $QoR_{12}(2)$ |  | $QoR_{ij}(3)$ |  |
| $QoR_5$ | $D_{min} + 4 * D_{scale}$ | $QoR_{12}(3)$ |  | $QoR_{ij}(4)$ |  |
| $\vdots$ | $\vdots$ | $\vdots$ |  | $\vdots$ |  |
| $QoR_\infty$ | No Protection Lightpaths | $QoR_{12}(\infty)$ |  | $QoR_{ij}(\infty)$ |  |

maximum recovery time of 20ms, no route of the lightpath satisfies the required recovery time. This is because the recovery time includes the time to propagate the notification about a failure occurence, and it takes more than 20ms whichever route is assigned to the primary lightpath.

Thus, we extend QoR such that the network administrator can specify the QoR class for each node pair $ij$. The network administrator first examines the smallest recovery time for node pair $ij$. It is determined by those including the propagation delay between node $ij$, node delay for lightpath switching, and so on. It is set as the recovery time for the highest class for node pair 12, which is represented as $QoR_{12}(1)$. Then, recovery times of the lower classes, $QoR_{12}(2)$, $QoR_{12}(3)$, … are determined. In the example of Table 2, the original QoR classes are defined by Eq. (1). First, $QoR_{12}(1)$ for node pair 12 is mapped to $QoR_3$. Then, the network administrator decides to map $QoR_{12}(n)$ to $QoR_{n+2}$. The network operator should make decisions for all node pairs. Then, the mapped $QoR_{ij}$ will be provided to end users, and the end user using node pair $ij$ chooses the prefered class from $QoR_{ij}(\cdot)$.

### 3.3 Modeling Recovery Times

In this subsection, we describe the behavior of the protection method in order to explain how to determine the recovery time. Figure 9 shows a primary lightpath $L$ is protected by several backup lightpaths $P_x$ ($1 \leq x \leq B$). Here, $B$ is the number of backup lightpaths for primary lightpath $L$, and $B$ is at most equal to the number of intermediate nodes that the primary lightpath traverses. We also define *segment* $x$ as a part of the primary lightpath between source and destination nodes of $P_x$ (denoted by $S_x$ and $D_x$, respectively). Using these notation, we describe the protection method and show how the recovery time is modeled in the protection method.

To provide QoR described in the above, we need to set up several backup lightpaths such that the maximum recovery time of each segment provided by backup lightpaths does not exceed a threshold value. For this purpose, we modify a SLSP (Short Leap Shared Protection) method proposed in [2]. In the original SLSP, several backup lightpaths are configured for each primary lightpath, so that any two neighboring backup lightpaths overlaps with each other (Figure 8). Unlike the shared protection method, SLSP can recover from a node failure. For example, if a failure occurs at node $D$, node $C$ switches the traffic to backup lightpath directly connected to node $H$.

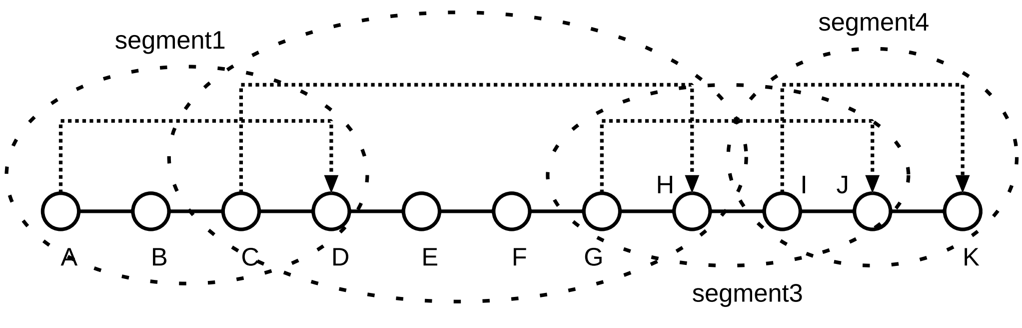


Figure 8: Illustrative example of SLSP

In [2], the quality metric is realized by specifying the maximum length of backup lightpath such that its length will be shorter than threshold. However, the SLSP only specifies the length of backup lightpath. In contrasts, we want to allow to specify the maximum recovery time for the primary lightpath $L$. Our QoR is realized by allocating backup lightpaths such that the maximum recovery time of each segment is smaller than same threshold. We also place two neighboring segments overlaps with each other for recovery from a single node failure.

We now model the recovery time using Figure 9. When a failure occurs at segment $x$, nodes next to the failed component send information to its previous nodes in order to notify the failure occurrence. When a failure information arrives at node $S_x$, $S_x$ reserves wavelengths on the prepared backup lightpath $P_x$ by sending reservation signal to $D_x$ through nodes $k, k+1, \ldots k+H_x$. Here, $H_x$ is a hop count of backup lightpath $P_x$. When the activation is completed, node $S_x$ switches the traffic on the primary lightpath onto $P_x$. As we see in the above, the recovery time when a failure occurs in the segment $x$ consists of three factors;

- Delay to propagate the failure information to node $S_x$
- Configuration time to reserve wavelengths at each node of backup lightpath $P_x$
- Switching time of the traffic on the failed primary lightpath to backup lightpath $P_x$

Thus, the maximum recovery time when a failure occurs in segment $x$ (denoted as $RT_x$) is represented as follows.

$$RT_x = \sum_{k=S_x}^{\alpha} d_{k(k+1)} + D_{node} \times (H_x + 1) + D_{conf}, \tag{3}$$

where $D_{node}$ is a wavelength reservation time consumed at each node along $P_x$, and $D_{conf}$ is the switching time at node $S_x$. In Eq. (3), $d_{ij}$ is the propagation delay between nodes $i$ and $j$. $\alpha$ is the maximum hop count that the failure information has to traverse in segment

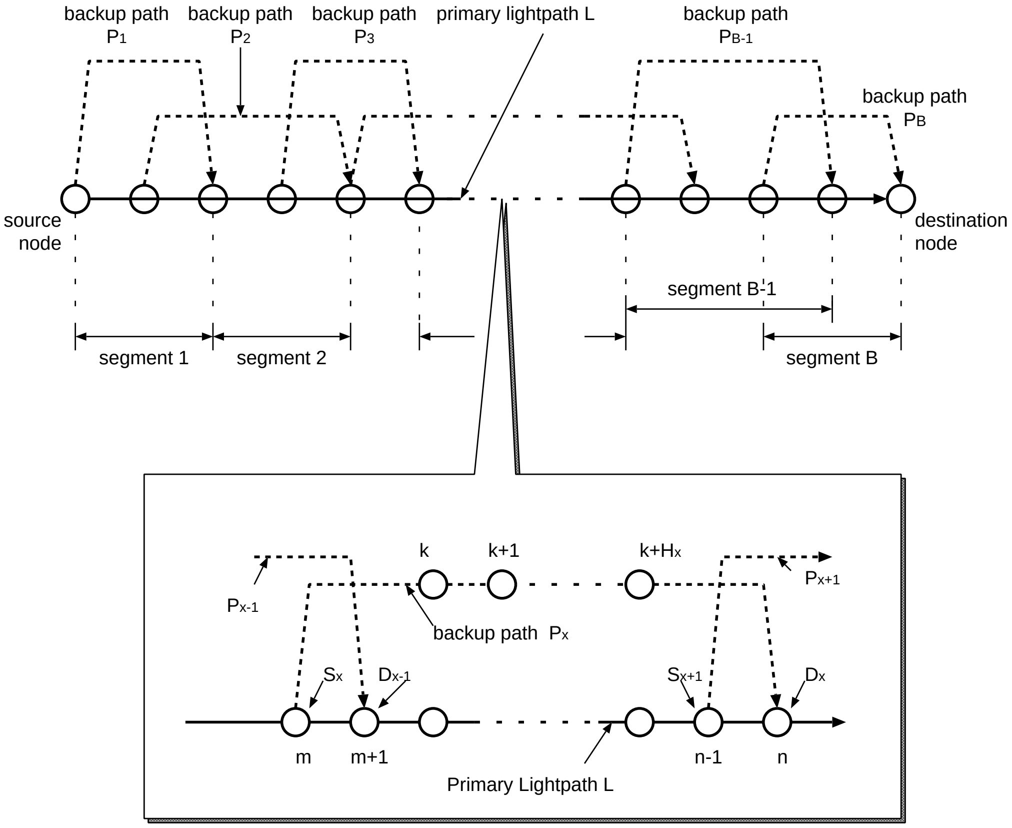


Figure 9: Primary Lightpath protected by Several Backup lightpaths $P_x$ $(1 \leq x \leq B)$

$x$. That is

$$\alpha = \begin{cases} D_x - 1, & D_x \leq S_{x+1}, \\ S_{x+1} - 1, & S_x < S_{x+1} < D_x, \end{cases} \tag{4}$$

The maximum recovery time for primary lightpath $L$, $RT_{max}(L)$, is the maximum of $RT_x$ for each segment $x$, and thus,

$$RT_{max}(L) = \max_{1 \leq x \leq B} \{RT_x\}. \tag{5}$$

# 4 Logical Topology Design Algorithms for Satisfying QoR Requirements

In this section, we describe three heuristic algorithms for designing logical topologies satisfying the QoR requirements. Our objective is to minimize the number of wavelengths in designing the logical topology, given that the traffic volume and QoR requirements for each node pair are prescribed. In essence, all of three algorithms work as follows.

Step 1: For each node pair $ij$, we set a metric $\beta_{ij}$ based on $QoR_{ij}(\cdot)$, which is used to determine the order of node pairs that lightpaths are assigned.

Step 2: In descending order of a metric $\beta_{ij}$, the route and wavelengths are assigned.

The route of backup lightpath is assumed to be configured on the shortest hop route between the source node $S_x$ and destination node $D_x$, and the route is disjoint with the link or node of its primary lightpath $L$ except $S_x$ and $D_x$. The reason for setting up backup lightpath based on the hop count is that the failure recovery time largely depends on the number of hops in our recovery model as shown in Eq. (5).

We next explain how the wavelength is allocated for backup lightpaths. It must be mentioned here that we do not consider wavelength conversion, and therefore, the same wavelength must be used for each lightpath (i.e., wavelength continuity constraints). When a backup lightpath is set up for protecting one segment of $L$, the same wavelength on $L$ must be assigned to the backup lightpath since the backup lightpath will be a part of primary lightpath after a failure (Figure 10). However, when source and destination nodes of the backup lightpath are identical to those of $L$, the backup lightpath does not require the same wavelength to be assigned with the primary lightpath. It is because the backup lightpath does not share any link with the primary lightpath in that case.

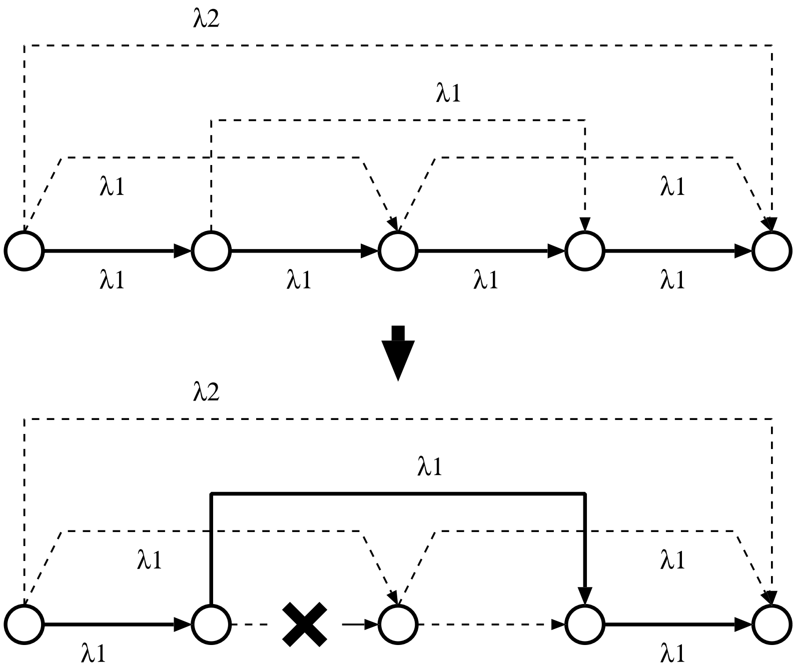


Figure 10: Wavelength Continuity

In what follows, we first describe two algorithms proposed in [10] in Subsections 4.1 and 4.2, and then propose our new algorithm in Subsection 4.3.

## 4.1 First–Fit Algorithm

A First–Fit algorithm first determines the routes of the primary lightpath and backup lightpaths. It becomes a combinational optimization problem to determine routes for the best set of a primary lightpath and backup lightpaths. To simplify the algorithm, the primary lightpath is routed by selecting the route with the smallest propagation delay between nodes, while the backup lightpath is set on the route of the minimum hop count on the link/node disjoint path.

After the routes of all the primary/backup lightpaths are determined, a wavelength is assigned to each lightpath based on a First–Fit (FF) policy [11]. The FF policy works as follows. When the algorithm discovers that several wavelengths $\{\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_n}; i_1 < i_2 < \ldots < i_n \}$ are available for the lightpath, we select the lowest index of the wavelength (i.e., $\lambda_{i_1}$ is selected ). Note that the wavelength assignment depends on whether the source and destination nodes of the backup lightpath are identical with those of the primary lightpath. That is,

- If the nodes are identical, a primary lightpath and the corresponding backup lightpath can be assigned with different wavelengths. Therefore, the algorithm first searches the available wavelength for the primary lightpath. Then, the wavelength for the backup lightpath is next determined independently of the wavelength assignment for its primary lightpath (see Figure 5(a)).
- If a backup lightpath protects the primary lightpath partially, a primary lightpath and the set of backup lightpaths must be assigned the same wavelength to satisfy the wavelength continuity constraint (Figure 5(b)).

### 4.2 Max–Shared Algorithm

In the Max–Shared algorithm, routes of the primary lightpath and a set of backup lightpaths are determined first, followed by the wavelength assignments to those lightpaths. The routing algorithm for primary and backup lightpaths are same to the First–Fit algorithm, i.e., finding the minimum propagation delay for primary lightpath, and the minimum hop counts for backup lightpaths. The difference from the First–Fit algorithm is in the wavelength assignments. In the Max–Shared algorithm, all wavelengths are examined for assigning both primary/backup lightpaths, and the best one is chosen. Throughout the trials of each wavelength, we count the number of links which are newly used for the backup lightpath, and set the counts as cost of the wavelength. Only in the case that backup lightpaths include a backup lightpath, whose source/destination nodes are identical to the primary lightpath, the wavelength of the backup lightpath is assigned independently to the primary lightpath. Note that we select a wavelength with minimum cost, if the several wavelengths are available for the backup lightpath.

The Max–Shared algorithm is expected to improve an effective usage of wavelength resources compared to the First Fit algorithm. This is because the Max–Shared algorithm assigns the wavelength to each set of primary and backup lightpaths from all the wavelengths to maximize the number of wavelengths they share with other lightpaths while the First–Fit algorithm does not try all wavelengths.

### 4.3 Logical Topology Design Algorithm based on Layered Graph

A layered graph consists of a set of wavelength graph $G_n (1 \leq n \leq W)$, each of which corresponds to the graph for wavelength $\lambda_n$ [3]. Wavelength graphs are independent of each other if the wavelength conversion is not allowed. The layered graph enables us to determine the route and wavelength of the lightpath at the same time, by calculating the shortest routes on each wavelength. Figure 11 shows an example of the layered graph where the number of wavelengths is set to $W$. In Figure 11, solid lines in each wavelength graph $G_n$ indicate that the wavelength $\lambda_n$ is free on the link, whereas the dotted lines do the wavelength is already used for primary or backup lightpaths. The metric for each edge of $G_n$ is the propagation delay of the corresponding link. To determine the wavelength to be assigned to each set of primary and backup lightpaths, we introduce a cost $C^n$ for each wavelength $\lambda_n$, which denotes the number of links where the wavelength $\lambda_n$ on the link is newly utilized by the set of primary and backup lightpaths. Our proposed algorithm works as follows.

Step 0: Initialize $w$, representing the number of wavelength necessary for constructing the logical topology, to 0.

Step 1: For each of possible lightpaths between nodes $i$ and $j$, do the following Steps 2

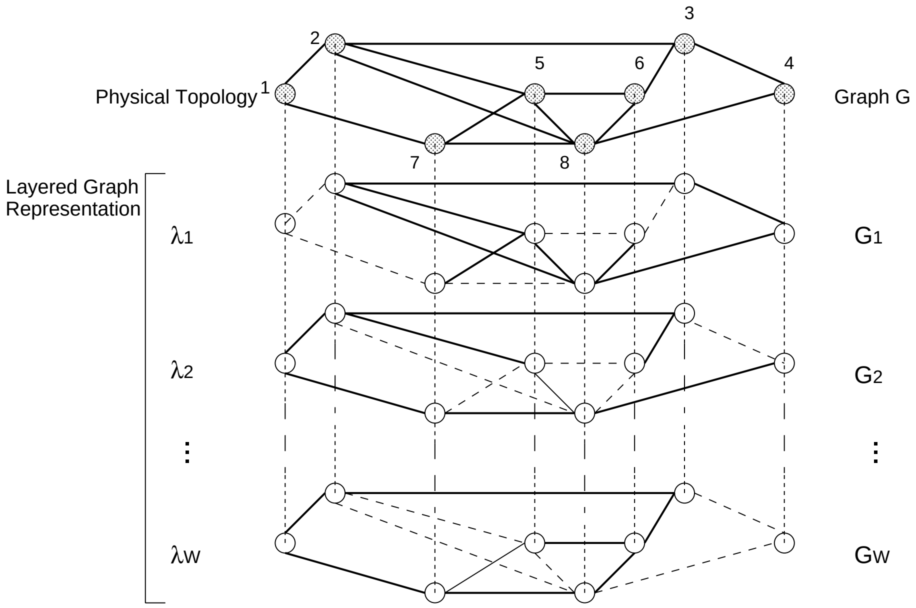


Figure 11: Example for Layered Graph: The number of wavelengths = $W$

through 4.

Step 2: Update $w$ by calculating the number of wavelengths which is already utilized at some links.

Step 3: From $\lambda_1$ to $\lambda_{w+1}$, do the following steps. (Assume that $\lambda_n$ is currently chosen in the following steps.)

Step 3.1: Check whether the route consisting of only unreserved wavelength exists between node pair $ij$ on graph $G_n$. If such a route does not exist, it means the primary lightpath cannot be set up. Then, go back to Step 3 and check the next wavelength on $G_{n+1}$. Otherwise, the primary lightpath, denoted by $L_{ij}$, can be set up on the route using $\lambda_n$, and update the metric of edges on $G_n$. That is, the corresponding links on $L_{ij}$ are deleted from $G_n$, and set the cost of the primary lightpath $C_p^n$ to the number of deleted links.

Step 3.2: Based on SLSP, we derive a set of backup lightpaths $\{P_1, P_2, \ldots, P_k\}$, each of which should satisfy $QoR_{ij}$ requirements. For this propose, the route of backup lightpaths are determined such that the backup lightpaths are disjoint to its primary lightpath $L_{ij}$ and the number of hop counts of the route is minimal. To satisfy these two conditions, we first calculate $C_r^n$, the cost for assigning wavelength $\lambda_n$ to the backup lightpath $P_r$ $(1 \leq r \leq k)$, and determine the set of backup lightpaths for $L_{ij}$.

Step 3.2.1: When the source node and destination node of $P_r$ is identical to those of $L_{ij}$, we tentatively assign $P_r$ to each wavelength $\lambda_i$ $(1 \leq i \leq w+1)$. If the backup lightpaths are partially configured at $L_{ij}$, we execute Step 3.2.2 only on graph $G_n$ because the backup lightpath partially protecting the primary lightpath must be assigned the same wavelength to the primary lightpath.

Step 3.2.2: If the backup lightpath $P_r$ can be set up on wavelength graph $G_e$, we set the cost of $P_r$ by counting the number of links, which are newly used on $G_e$, and set it to $C_e$. After checking all wavelengths (i.e., $G_1$ through $G_{w+1}$), select $e'$ where the cost $C_{e'}$ of corresponding $G_{e'}$ is minimum. Then, set $C_{e'}$ to $C_r^n$.

Step 3.3: Set $C^n \leftarrow C_p^n + \sum_{r=1}^{k} C_r^n$. Here, $C^n$ is the cost of wavelength $\lambda_n$ for setting up both primary/backup lightpaths between nodes $i$ and $j$. Go back to Step 3.

Step 4: Select $a$ such that $C^a$ is a minimum value of $\{C^1, C^2, \ldots, C^{w+1}\}$, and assign wavelength $\lambda_a$ to $P_a$ and $P_r$ which is partially protecting the $P_a$. Then, $\lambda_{e'}$ which is precalculated at Step 3.2.2 is assigned to path protection backup lightpath.

The algorithm calculates the cost of assigning the primary and backup lightpaths for each wavelength in Step 3.1 and Step 3.2, respectively. In Step 3.3, we calculate the cost $C_r^n$ for each backup lightpath $r$ on $\lambda_n$, where the cost means the number of newly utilized wavelength resources. Step 3 determines the actually used wavelength that minimizes the cost of assigning both primary and backup lightpaths, and set up the lightpaths using $\lambda_a$. Note that the above algorithm counts the number of wavelength necessary, $w$. However when the number of wavelengths is set to $W$, Step 3.1 through 3.4 are examined from $\lambda_1$ to $\lambda_W$.

# 5 Numerical Evaluations and Discussions

## 5.1 Network Models

We use a 14–node NSFNET model (Figure 12) and a traffic matrix (Table 3) given in [12] to evaluate three algorithms. The traffic matrix in [12] is given in relative values of the amount of traced traffic on NSFNET in 1992. Hence, we introduce a traffic scale factor $\gamma$ and give the traffic matrix multiplied by $\gamma$ as an actual traffic demand, assuming that the unit of the traffic matrix shown in Table 3 is Gbps. The bandwidth of each wavelength

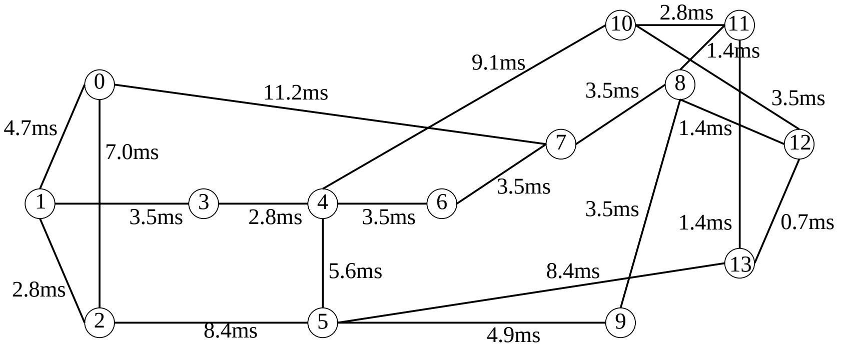


Figure 12: 14–Node NSFNET

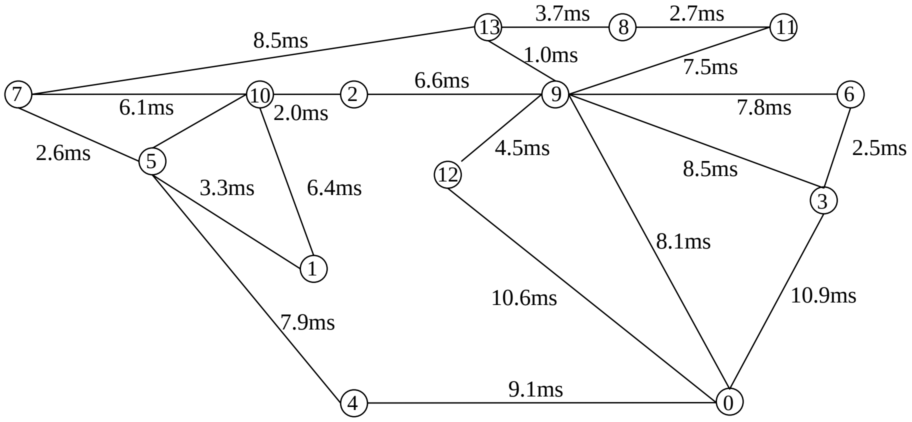


Figure 13: 14–Node Random Network

is set to 10Gbps and a connection, whose requested bandwidth is greater than 10Gbps, is assigned the multiple lightpaths enough to carry the traffic. When two or more lightpaths are assigned to the connection, we set routes of these lightpaths on the same routes.

We also employ a randomly generated network, where the number of links of the network is set to 21 and they are placed randomly on the 14–node network. Note that the numbers of links and nodes are same to NSFNET. The propagation delay for the link is also given randomly ranging from 0.7ms and 11.2ms, which are respectively the shortest and the longest propagation delays of links in the original NSFNET. A traffic matrix for the network is also randomly selected between 0.0004 and 21.030, which is the minimum and maximum values in Table 3.

In the following subsections, we will use the values of $D_{min}$ = 10ms, $D_{scale}$ = 2ms, $D_{node}$ = 1ms, and $D_{conf}$ = 0ms.

Table 3: Traffic Matrix for NSFNET

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.000 | 0.109 | 0.206 | 0.014 | 0.045 | 0.004 | 0.043 | 0.145 | 0.051 | 0.010 | 0.007 | 0.008 | 0.000 | 0.033 |
| 1 | 1.171 | 0.000 | 0.856 | 0.062 | 1.112 | 0.777 | 0.362 | 1.579 | 0.366 | 1.661 | 0.203 | 3.781 | 0.483 | 1.319 |
| 2 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| 3 | 0.031 | 0.341 | 1.364 | 0.000 | 0.190 | 0.060 | 0.070 | 0.288 | 0.200 | 0.326 | 0.307 | 0.669 | 0.008 | 0.401 |
| 4 | 0.028 | 6.751 | 1.902 | 0.343 | 0.000 | 0.403 | 1.077 | 6.222 | 2.402 | 1.792 | 0.045 | 7.903 | 0.997 | 0.529 |
| 5 | 0.000 | 0.581 | 0.342 | 0.552 | 0.340 | 0.000 | 0.261 | 0.268 | 0.087 | 0.387 | 0.004 | 0.084 | 0.006 | 0.248 |
| 6 | 0.175 | 2.202 | 10.231 | 0.447 | 2.203 | 0.790 | 0.000 | 11.410 | 1.982 | 2.195 | 0.078 | 7.140 | 0.033 | 3.284 |
| 7 | 0.239 | 6.384 | 21.030 | 0.852 | 2.821 | 0.266 | 9.708 | 0.000 | 4.395 | 3.300 | 1.137 | 4.863 | 0.553 | 1.385 |
| 8 | 0.645 | 1.893 | 3.735 | 0.600 | 2.499 | 0.681 | 2.506 | 6.102 | 0.000 | 3.962 | 1.452 | 12.750 | 2.334 | 0.076 |
| 9 | 0.005 | 3.529 | 1.026 | 0.373 | 2.234 | 0.948 | 0.498 | 5.708 | 0.684 | 0.000 | 0.630 | 1.764 | 0.591 | 0.076 |
| 10 | 0.010 | 0.102 | 0.313 | 0.169 | 0.024 | 0.006 | 0.081 | 0.145 | 0.058 | 0.712 | 0.000 | 0.084 | 0.006 | 0.050 |
| 11 | 0.128 | 2.615 | 0.100 | 0.594 | 2.486 | 0.132 | 0.549 | 4.057 | 2.953 | 2.237 | 1.050 | 0.000 | 0.101 | 0.054 |
| 12 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 |
| 13 | 0.073 | 2.909 | 1.363 | 0.989 | 3.561 | 1.207 | 0.644 | 2.879 | 0.467 | 0.000 | 0.399 | 0.000 | 1.075 | 0.000 |

Table 4: Traffic Matrix for Random Network

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|---:|
| 0 | 0.000 | 6.014 | 16.019 | 16.596 | 7.874 | 7.979 | 9.556 | 20.655 | 17.433 | 16.887 | 16.318 | 3.662 | 8.016 | 21.928 |
| 1 | 10.809 | 0.000 | 8.875 | 16.940 | 17.114 | 4.149 | 10.389 | 1.429 | 12.390 | 9.286 | 14.597 | 0.614 | 9.435 | 23.283 |
| 2 | 6.535 | 18.131 | 0.000 | 1.331 | 6.372 | 10.558 | 21.717 | 12.767 | 17.530 | 5.591 | 20.742 | 17.462 | 2.246 | 4.555 |
| 3 | 10.349 | 18.561 | 22.590 | 0.000 | 8.741 | 16.489 | 9.399 | 17.612 | 23.805 | 2.514 | 12.137 | 10.195 | 18.315 | 0.528 |
| 4 | 19.477 | 8.912 | 1.138 | 4.912 | 0.000 | 8.195 | 22.045 | 13.420 | 23.898 | 18.793 | 14.354 | 21.615 | 7.561 | 22.260 |
| 5 | 3.207 | 18.679 | 15.722 | 19.825 | 13.611 | 0.000 | 2.072 | 14.386 | 12.201 | 1.189 | 21.251 | 11.976 | 9.178 | 21.057 |
| 6 | 4.866 | 21.311 | 21.628 | 23.178 | 12.215 | 17.105 | 0.000 | 8.090 | 3.729 | 12.394 | 6.662 | 1.775 | 16.190 | 20.936 |
| 7 | 10.944 | 6.544 | 18.552 | 8.881 | 4.804 | 12.135 | 3.561 | 0.000 | 20.522 | 7.960 | 7.548 | 12.970 | 12.723 | 19.745 |
| 8 | 14.156 | 0.354 | 22.097 | 23.330 | 11.787 | 2.964 | 11.021 | 9.415 | 0.000 | 2.142 | 23.233 | 16.897 | 0.608 | 2.962 |
| 9 | 5.291 | 21.642 | 19.109 | 21.477 | 18.579 | 20.430 | 18.397 | 3.511 | 5.311 | 0.000 | 13.577 | 15.642 | 23.244 | 10.099 |
| 10 | 13.978 | 6.792 | 13.446 | 17.077 | 16.913 | 17.978 | 17.428 | 15.011 | 7.688 | 5.215 | 0.000 | 17.971 | 18.705 | 5.007 |
| 11 | 20.109 | 8.318 | 21.900 | 11.093 | 1.657 | 3.191 | 8.736 | 20.762 | 15.044 | 3.315 | 7.572 | 0.000 | 23.817 | 6.822 |
| 12 | 12.880 | 13.394 | 12.840 | 2.504 | 23.489 | 17.194 | 9.293 | 3.315 | 10.272 | 2.206 | 21.289 | 18.076 | 0.000 | 7.593 |
| 13 | 4.977 | 13.667 | 1.564 | 14.059 | 18.670 | 12.049 | 22.373 | 16.570 | 23.139 | 0.030 | 10.137 | 22.251 | 11.169 | 0.000 |

## 5.2 Evaluation Results and Discussions

We first show the number of necessary wavelengths in each algorithm when every node pair $ij$ requests the same $QoR_{ij}$. More specifically, in the current example, the network administrator prepares $QoR_{ij}$ classes dependent on node pair $ij$. For example, assume the case of node pair $3, 4$ in NSFNET (Figure 12). If the primary lightpath is set to the route $[3 \rightarrow 4]$ and a backup lightpath to $[3 \rightarrow 1 \rightarrow 2 \rightarrow 5 \rightarrow 4]$ between node pair $3, 4$, the maximum recovery time is 6.8ms. If lightpaths are set on different routes, the maximum recovery time will be more than 6.8ms. Therefore, 6.8ms is the minimum time of the maximum time to be guaranteed for node pair $3, 4$. Here, if $D_{min}$ and $D_{scale}$ are set to 5ms and 1ms, respectively, the maximum recovery time guaranteed in $QoR_2$ is 6ms and that in $QoR_3$ is 7ms. Accordingly, $QoR_{34}(1)$ is set to $QoR_2$.

In the current example, however, all node pairs are assumed to request the identical class to simply show the relationship between $QoR_{ij}$ and the number of necessary wave-

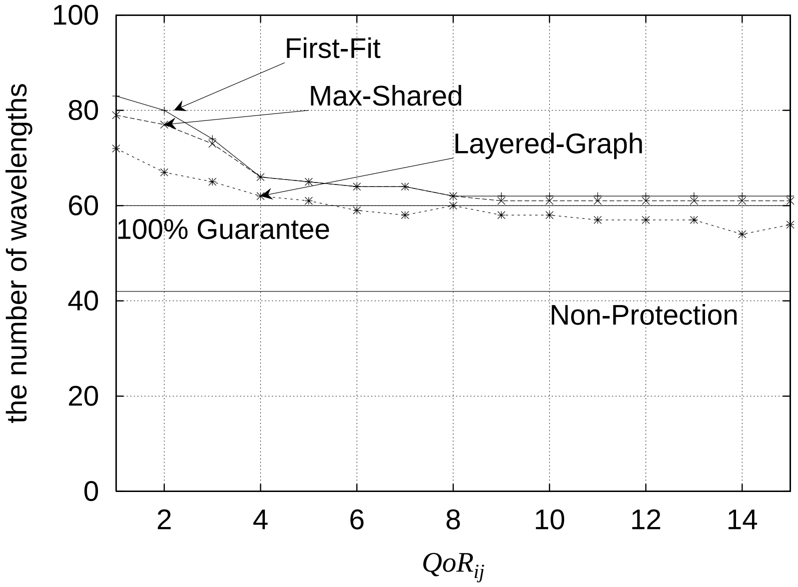


Figure 14: $QoR_{ij}$ vs the Number of Wavelengths in NSFNET: $\gamma = 1$

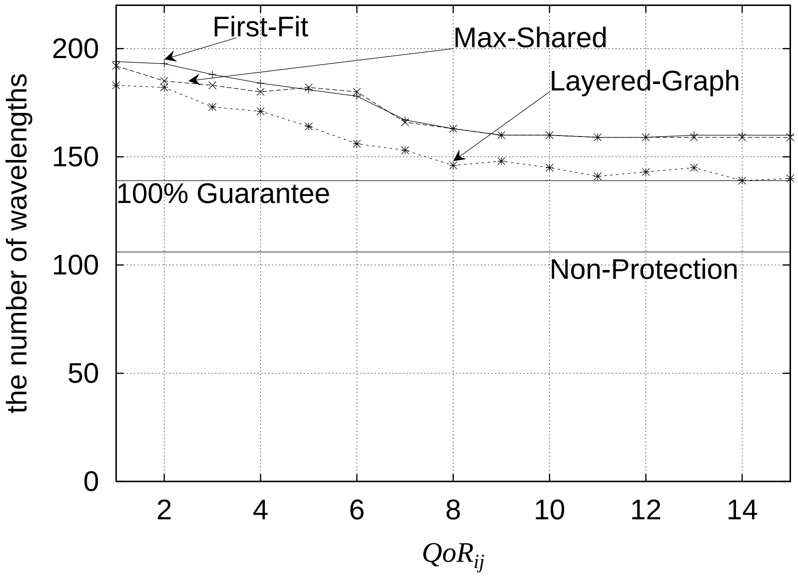


Figure 15: $QoR_{ij}$ vs the Number of Wavelengths in Random Network: $\gamma = 1$

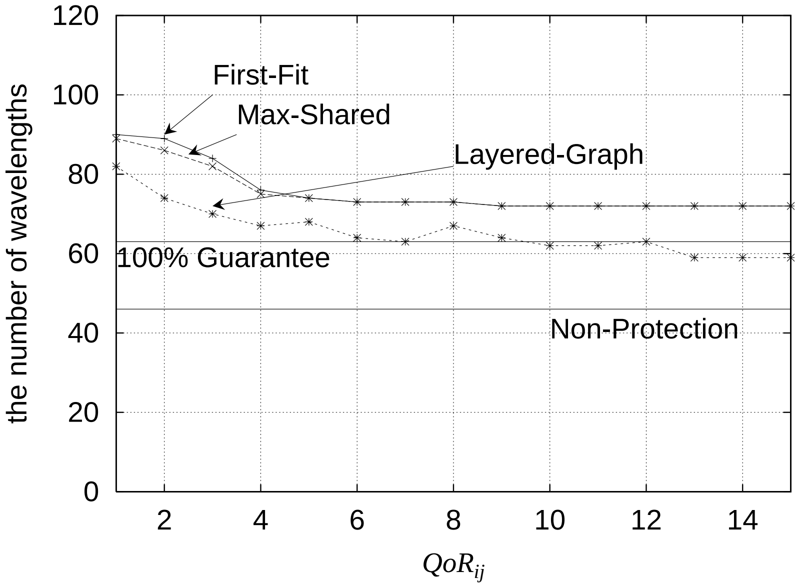


Figure 16: $QoR_{ij}$ vs the Number of Wavelengths: $\gamma = 2$

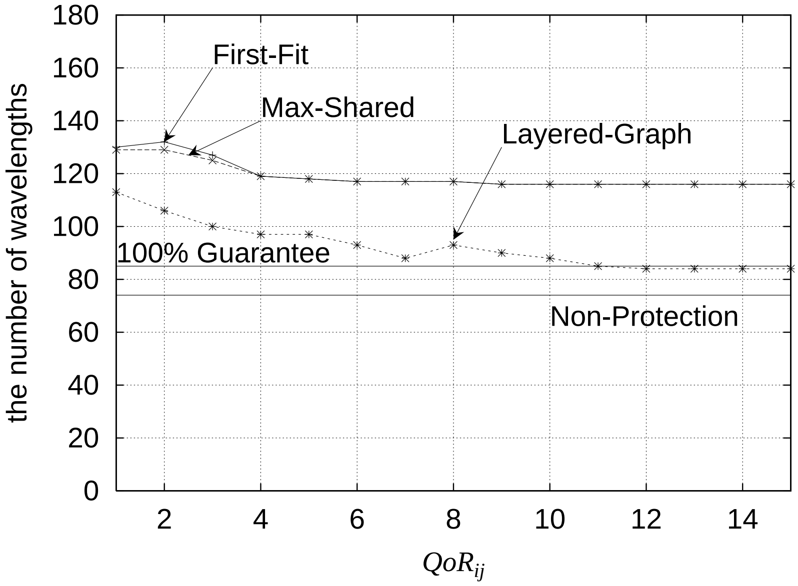


Figure 17: $QoR_{ij}$ vs the Number of Wavelengths: $\gamma = 5$

lengths in each algorithm. The horizontal axis in Figure 14 shows the class number that all node pairs request. The vertical axis means the required number of the wavelengths for setting up all the primary/backup lightpaths for fulfilling the requests. In obtaining the figure, we use the network model of NSFNET (Figure 12), and the traffic scale factor $\gamma$ of 1. We can observe that our proposed algorithm, which is based on the layered graph, utilizes wavelength resources more effectively than other algorithms. Especially when $QoR_{ij}$ is high (e.g., $QoR_{ij} = 1$ or 2), the layered graph algorithm shows a better usage of wavelength resources. The reason is as follows. When $QoR_{ij}$ is high, more backup lightpaths should be configured over the network to realize the required recovery times. Then, the layered graph algorithm can determine routes for each primary and backup lightpaths to reduce the additional amount of wavelength resources. Note that a solid lines without points show the result of the case where no backup lightpath is prepared for primary lightpaths (labelled as Non–Protection in each figure), and the case where only one backup lightpath is configured to each primary lightpath based on the layered

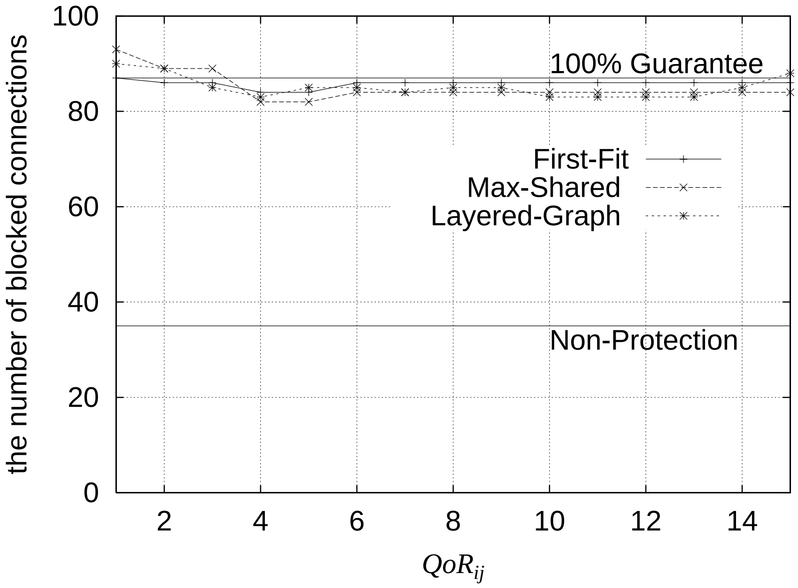


Figure 18: The Number of Blocked Connections: $W = 20$

graph, which guarantees 100% reliability (labelled as 100% Guarantee in each figure). The number of necessary wavelengths with our QoR is at most 100% more than those with no protection in this experiment. Moreover, the number of necessary wavelengths for our three algorithms is at most 50% more than the result of 100% guarantee. In Figures 14, 15, 16, and 17, the number of necessary wavelengths for the 100% guarantee is more than those by the layered graph algorithm at lower $QoR_{ij}$. This is owing to the following fact. Even for the lower $QoR_{ij}$, backup lightpaths configured by the layered graph algorithm are slightly more than those by the 100% guarantee. As a result, the layered graph algorithm requires the lower number of wavelengths, compared with the 100% guarantee case. This tendency is also observed when algorithms are applied to the randomly generated network (Figure 15).

We next show the evaluation results by increasing the traffic volume, $\gamma = 2$ in Figure 16 and $\gamma = 5$ in Figure 17, respectively. Both figures again show that the layered graph algorithm gives the best effective usage on wavelength resources among three algorithms.

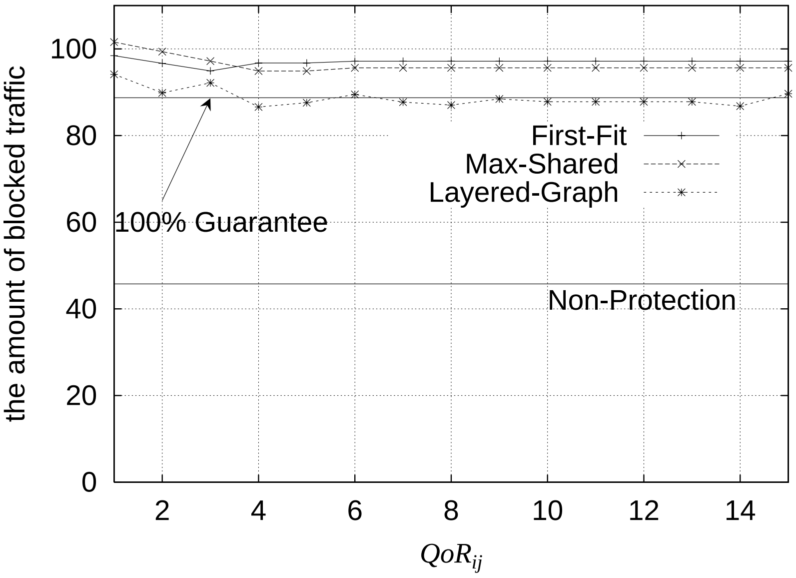


Figure 19: The Amount of Blocked Traffic: $W = 20$

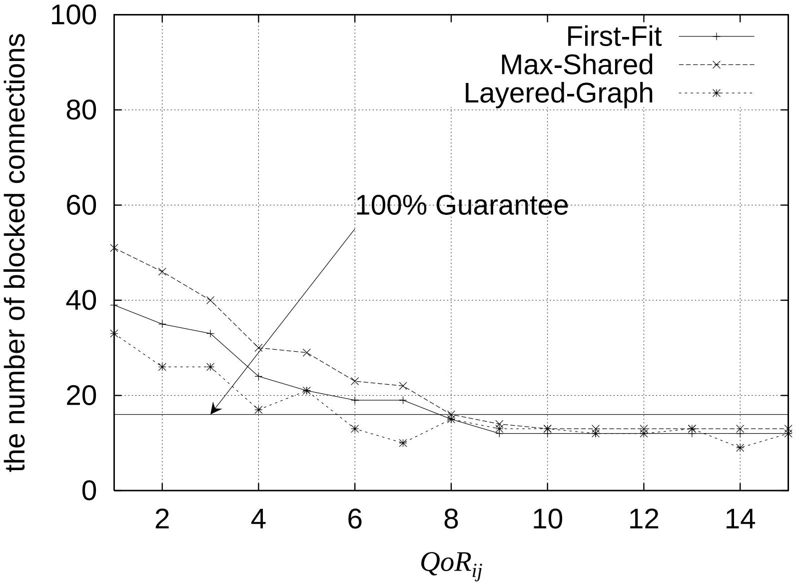


Figure 20: The Number of Blocked Connections: $W = 50$

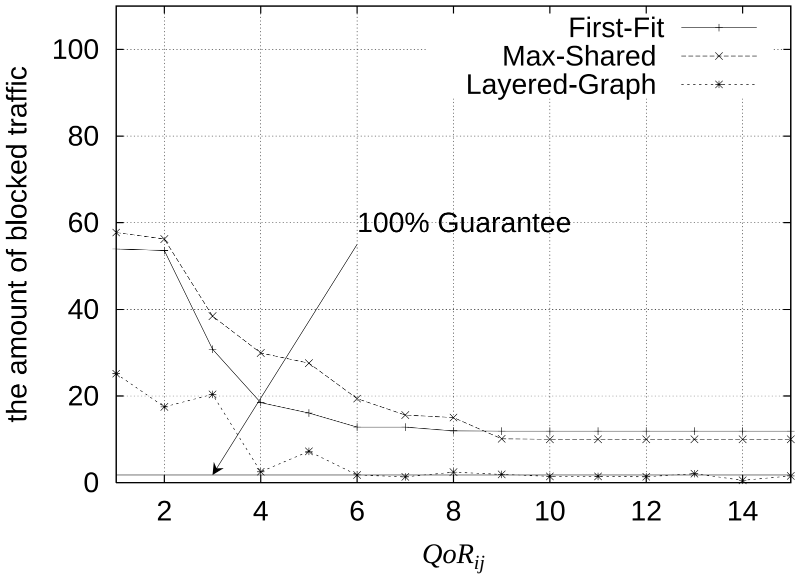


Figure 21: The Amount of Blocked Traffic: $W = 50$

Next, we limit the number of wavelengths, $W$, to 20. $QoR_{ij}$ is configured same as in previous evaluations. The number of blocked connections due to a lack of wavelength resources, and the total amount of traffic volume on the blocked connections are compared in Figures 18 and 19, respectively. The NSFNET model with $\gamma = 1$ is used in obtaining these figures. A significant difference is not observed among three algorithms when $W = 20$. However, if the number of wavelengths is set to 50, the advantage of the layered-graph algorithm becomes significant as shown in Figures 20 and 21, which show the result of the number of blocked connections and the amount of blocked traffic, respectively. The reason is explained as follows. As the number of available wavelengths increases, it becomes easy to find wavelength resources for the backup lightpaths to be shared with other backup lightpaths. Therefore, more wavelengths can be shared as the number of wavelengths is increased. That is, the advantage of the layered graph algorithm becomes remarkable as the the number of wavelengths becomes large. Here, we should note that there is no blocking for the case of no backup lightpaths when the number of wavelength was set to 50.

# 6 Conclusion

In this thesis, we have introduced QoR (Quality of Reliability), which is a new concept of QoS with respect to the reliability in the WDM network. Our QoR guarantees the maximum recovery time according to the request by users, in addition to the 100% existence of backup lightpaths. We then extend our QoR for specifying QoR for each node pair $ij$ as $QoR_{ij}$. Based on $QoR_{ij}$, we have proposed a heuristic algorithm to design a logical topology with a protection method satisfying $QoR_{ij}$ requirements. The objective of our proposed algorithm is to minimize the number of necessary wavelengths to carry the overall traffic and provide a functionality of fault tolerance with QoR requirements. Numerical results have shown that our proposed algorithm based on the layered graph can utilize wavelength resources more effectively than other algorithms, as the requested traffic volume becomes large. We have also shown that it can carry more connections against the limited number of wavelengths.

Several topics are still left for future work. One of them is to obtain some guidelines to determine the classification of QoR and specification of $QoR_{ij}$, considering the network environment. The other future work is as follows. In our thesis, we have assumed that the traffic between a node pair requests identical $QoR_{ij}$, while in the actual network, different class of $QoR_{ij}$ might be requested between the same node pair. Therefore, it is necessary to extend our work to obtain a logical topology design algorithm with multiple classes of $QoR_{ij}$ even for same node pair $ij$. The upper layer of the WDM layer is another interest of our future work. In this thesis, we have considered the fault tolerance functionality with respect to the WDM layer solely. However, for example, the effect of the restoration functionality of IP layer should also be considered for building highly reliable networks.

# Acknowledgements

I would like to express my sincere appreciation to Professor Masayuki Murata of Osaka University, who introduced me to the area of photonic networks including the subjects in this thesis.

My special thanks are due to Research Assistant Shin'ichi Arakawa of Osaka University. I appreciate his valuable and constant advice. His conscientious coaching was always helpful.

All works of this thesis would not have been possible without them. It gives me great pleasure to acknowledge their assistance. They have been constant sources of encouragement and advice through my studies and preparation of this manuscript.

I am also indebted to Professor Hideo Miyahara, Assistant Professor Naoki Wakamiya, Research Assistant Hiroyuki Ohsaki, and Research Assistant Go Hasegawa of Osaka University who gave me helpful comments and feedbacks.

Finally, I thank all students of Advanced Network Architecture laboratory and Multimedia Information System Laboratory, colleagues in the Department of Informatics and Mathematical Science of Osaka University, and my friends for their support.

# References

[1] S. Ramamurthy and B. Mukherjee, “Survivable WDM mesh networks, part I – Protection,” in *Proceedings of IEEE INFOCOMM ’99*, pp. 744–751, March 1999.

[2] P.-H. Ho and H. T. Mouftah, “A framework of a survivable optical Internet using short leap shared protection (SLSP),” in *Proceedings of 2001 IEEE Workshop on High Performance Switching and Routing*, pp. 21–25, May 2001.

[3] V. Anand and C. Qiao, “Static versus dynamic establishment of protection paths in WDM networks,” in *Proceedings of IEEE INFOCOM 2001*, April 2001.

[4] O. Gerstel and G. Sasaki, “Quality of protection (QoP): A quantitative unifying paradigm to protection service grades,” in *Proceedings of Opticomm 2001*, April 2001.

[5] C. V. Saradhi and C. S. R. Murthy, “Routing differentiated reliable connections in WDM optical networks,” in *Proceedings of Opticomm 2001*, August 2001.

[6] M. Kodialam and T. V. Lakshman, “Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information,” in *Proceedings of IEEE INFOCOM 2000*, pp. 902–911, March 2000.

[7] G. Mohan and A. K. Somani, “Routing dependable connections with specified failure restoration gurantees in WDM networks,” in *Proceedings of IEEE INFOCOM 2000*, pp. 1761–1770, March 2000.

[8] R. Ramaswami and K. N. Sivarajan, “Design of logical topologies for wavelength-routed all-optical networks,” in *Proceedings of IEEE INFOCOM ’95*, pp. 1316–1325, April 1995.

[9] B. Mukherjee, D. Banerjee, S.Ramamurthy, and A. Mukherjee, “Some principles for designing a wide-area WDM optical network,” *IEEE/ACM Transactions on Networking*, vol. 4, pp. 684–695, October 1996.

[10] J. Katou, S. Arakawa and M. Murata, “Design method of logical topologies in WDM network with quality of protection,” in *Proceedings of Workshop on OPTICAL NETWORKING*, November 2001.

[11] H. Zang, J. P. Jue, and B. Mukherjee, “A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks,” *Optical Network Magazine*, pp. 47–60, January 2000.

[12] R. Ramaswami and K. N. Sivarajan, “Design of logical topologies for wavelength-routed optical networks,” *IEEE Journal on Selected Areas in Communications*, vol. 14, pp. 840–851, June 1996.