Survivability in the Optical Internet Using the Optical Burst Switch

Seunghun Oh, Younghan Kim, Myungsik Yoo, and Hyun Ha Hong

Due to its salient features, the optical burst switch is becoming a key technology for the optical Internet. Within this technology, the survivability issue in the optical Internet has to be addressed because a simple failure causes severe damage to the huge amount of data carried in optical fiber. In this paper, we introduce a restoration procedure that can provide good survivability in the optical burst switch (OBS)-based optical Internet. OBS restoration can survive various types of network failure while maintaining good network performance. We propose novel restoration mechanisms, namely, "temporary Label Switched Path (LSP)" and "bossy LSP," to enhance restoration time and network utilization. The simulation results verify that the proposed OBS restoration achieves good network performance and provides good network connectivity as well.

Manuscript received Sept. 21, 2001: revised Feb. 18, 2002.

This work was supported in part by the Korean Science and Engineering Foundation (KOSEF) through OIRC project.

Seunghun Oh (phone: +82 2 814 0951, e-mail: Jake93@dcn.ssu.ac.kr), Younghan Kim (e-mail: yhkim@dcn.ssu.ac.kr), and Myungsik Yoo (e-mail: myoo@e.ssu.ac.kr) are with Soong-Sil University, Seoul, Korea.

Hyun Ha Hong (e-mail: hhhong@etri.re.kr) is with ETRI, Daejeon, Korea.

I. INTRODUCTION

Switching techniques are being developed to provide the internet with wider capacity, more flexibility, and faster networks. The rapid advance in optical technology is accelerating research on optical switching technology, which is a crucial part of the optical Internet. There are currently three switching techniques that can be applied to the optical Internet. The first one, the optical circuit switch (OCS) provides a dedicated circuit (wavelength) between two end-points for connection-oriented communication [1]. With the second one, the optical packet switch (OPS), each optical packet, which is appended with the routing information, is transmitted along a route that is calculated in each hop according to the information within the optical packet [2], [3]. The OCS usually results in poor resource utilization, and the OPS is difficult to implement because of the technical limitations on optics. The third technique is the optical burst switch (OBS). By the virtue of its features, the OBS can improve the poor utilization of the OCS by statistically multiplexing data bursts and at the same time, it can attenuate the technical limitations of the OPS (such as optical random access memory and fast switching time of the optical switch [1], [4]).

As the optical Internet [5] has been positioned in the infrastructure of the next generation Internet [6], the issue of survivability has become more and more important. A huge amount of data traffic is carried by a single fiber, and that fiber is susceptible to faults, for example, fiber cuts. Even a single network element fault in an optical network brings about multiple session errors in a higher layer and thus can trigger different alarming messages and many restoration procedures at a higher layer [7]. This causes network service interruption and a heavy burden on the network. Generally, the layered architecture of the optical Internet has been developed on the basis of an IP/ATM/SONET/WDM hierarchy with a dependency on the SONET layer for optical restoration. However, this architecture has unnecessarily overlapped functions because of the independence of the layers from each other, and because it is too slow to scale for a large volume of traffic. Because the development of optical technology makes it possible for the WDM optical layer to include functions of higher layers, the simple architecture of "IP/WDM," which is more scalable and more efficient, has attracted more attention and is likely to be adapted for the optical Internet [8], [9]. Due to its advantages over the OCS and OPS, the OBS is the one of the most feasible technologies for that simple hierarchical architecture.

This paper focuses on the survivability of the optical Internet and in particular, introduces restoration procedures specific to the OBS. By taking advantage of the Multi-protocol Labeled Switch (MPLS) control plane [11], we apply an MPLS restoration scheme [12]-[14] to our approach. We demonstrate that the features of the OBS can efficiently enhance the survivability of the optical Internet by increasing the possibility of fault localization [7], [10].

The rest of the paper is organized as follows. In section II, we present the general concept of restoration in both optical networks and MPLS networks as background for the restoration. section III introduces the restoration procedures based on the OBS as well as the different kinds of network fault detection methods. In section III, we present the simulation results of the OBS restoration in terms of restoration time and the loss rate. Finally, we conclude the paper in section IV.

II. RESTORATION

Restoration can be distinguished in different ways from different viewpoints. Restoration in a network is classified as 'Protection' or 'Dynamic Recovery' depending on the time when the backup path is prepared. Under Protection, when a network is deployed, a backup path (or protection path) is calculated and established to protect the working path; a network fault will be restored through this pre-planned path. While the original path carrying traffic is called a working path, the path that the traffic will be switched over to is called a backup path or protection path. With this scheme it is difficult to restore multiple network failures or a node failure. Under Dynamic Recovery, on the other hand, the backup path is calculated and established just after the network fault is detected. Dynamic Recovery has better network utilization than Protection and is able to restore both a node failure and multiple network failures, but it takes too long to efficiently serve delay-sensitive applications [15].

Depending on the location of the nodes responsible for surviving a failure, restoration can be classified as local restoration or global restoration [12]. In local restoration the nodes on both sides of the fault point have responsibility for the restoration, which is transparent to other nodes on the working path. On the other hand, in global restoration the two endpoints (the source and destination nodes) on the working path replace the whole path affected by the network failure with the backup path, which is disjoint from the working path. Global restoration takes longer and consumes more resources. To achieve better resource utilization and faster restoration, it is desirable to use local restoration as much as possible. In the OBS optical Internet, we call local restorations link-level restoration and global restorations path-level restoration.

Protection is classified as 'dedicated' or 'shared' depending on whether the backup path's resource is shared with another backup path [12]. Dedicated Protection needs N backup paths, which are N dedicated resources, in order to protect N working paths. Shared Protection allows backup paths corresponding to multiple working paths to share common resources for protection, which results in better resource utilization.

In the following two subsections, we describe restoration in optical networks and IP (MPLS) networks.

1. Restoration in Optical Networks

Optical networks are generally WDM-based and consist of two sub-layers: the optical channel layer (OCh) and the optical multiplex section layer (OMS). Therefore, restoration in optical networks also consists of an OCh resilient scheme and OMS resilient scheme [16], which are called path-restoration and line-restoration, respectively. The difference between the OCh resilient scheme and the OMS resilient scheme is the granularity of the restored traffic. While the former restores the lightpath individually, the latter restores all the lightpaths on the fault link. Either Protection or Dynamic Recovery can be applied to both schemes [17].

A. Dynamic Optical Recovery Schemes

With the occurrence of an optical channel failure, Dynamic Recovery in the OCh layer restores the lightpath affected by the failure by replacing it with the backup lightpath, which is dynamically established after the failure is detected. The backup lightpath can be obtained in either a distributed or a centralized way. In the centralized way, the managing center maintains the network states and calculates the route based on the state information. Upon receiving the restoration request message, it delivers the routing information for a backup lightpath to the requesting node. In the distributed way, the source and destination nodes at the ends of a fault channel find the backup lightpath dynamically [16], [18].

Dynamic Recovery in the OMS layer is executed by finding the backup line, which is locally disjointed from the fault-affected link. It is the node at the link failure that executes the restoration, so it is better to calculate the backup path dynamically in a distributed way than in a centralized way [17].

B. Optical Protection Schemes

Protection in the OCh layer and the OMS layer is called path Protection and line Protection (or link Protection), respectively. The backup path or line (link) can be either shared or dedicated. A 1+1 Protection represents the dedicated Protection. A 1:N Protection represents the shared Protection. When a network failure occurs, the protection path is activated with the setting of each wavelength on each node along a pre-planned route using a signal protocol, and then the protection procedure is completed by switching over the traffic on the affected path to the activated backup path. One of the major problems of the shared backup path is contention for the shared path when multiple faults occur: An extra signal protocol is necessary for resolving contentions.

C. Restoration Schemes Specific to Network Topology

This subsection describes some restoration schemes that are based on the various schemes introduced in previous subsections A and B according to the types of network topologies to be restored: point-to-point network, ring topology, and mesh network [16], [19].

Protection in a point-to-point network is based on the line layer, and 1+1 and 1:1 line Protection are examples. Fig. 1(a) illustrates the 1+1 line Protection where the same traffic is transmitted through both the working line and the backup line. The node on the other side selects one of them by monitoring the quality of the signal.

Several ring-based restoration schemes for the optical layer have been developed on the basis of the self-healing ring (SHR) in the SONET layer [16]. Among them, the UPSR (uni-directional path switched ring) is 1+1 Protection as in Fig. 1(b), and shared protection ring/2 (SPRING/2) and shared protection ring/4 (SPRING/4) are ring-based shared restorations. Fig. 1(b) illustrates the UPSR where the link between two nodes consists of two fibers: the working fiber and the protection fiber. This restoration is executed as 1+1 Protection by sending the same traffic through the working fiber and the protection fiber, but in opposite directions. One of them is selected according to the quality of the signal. Fig. 1(c) illustrates SPRING/4, which consists of two working fibers and two protection fibers. With a link failure, two nodes at the link failure restore the traffic by connecting the working fiber to the protection fiber and transmitting traffic from the working fiber to the protection fiber. SPRING/2 is nearly the same as SPRING/4 except that it con-

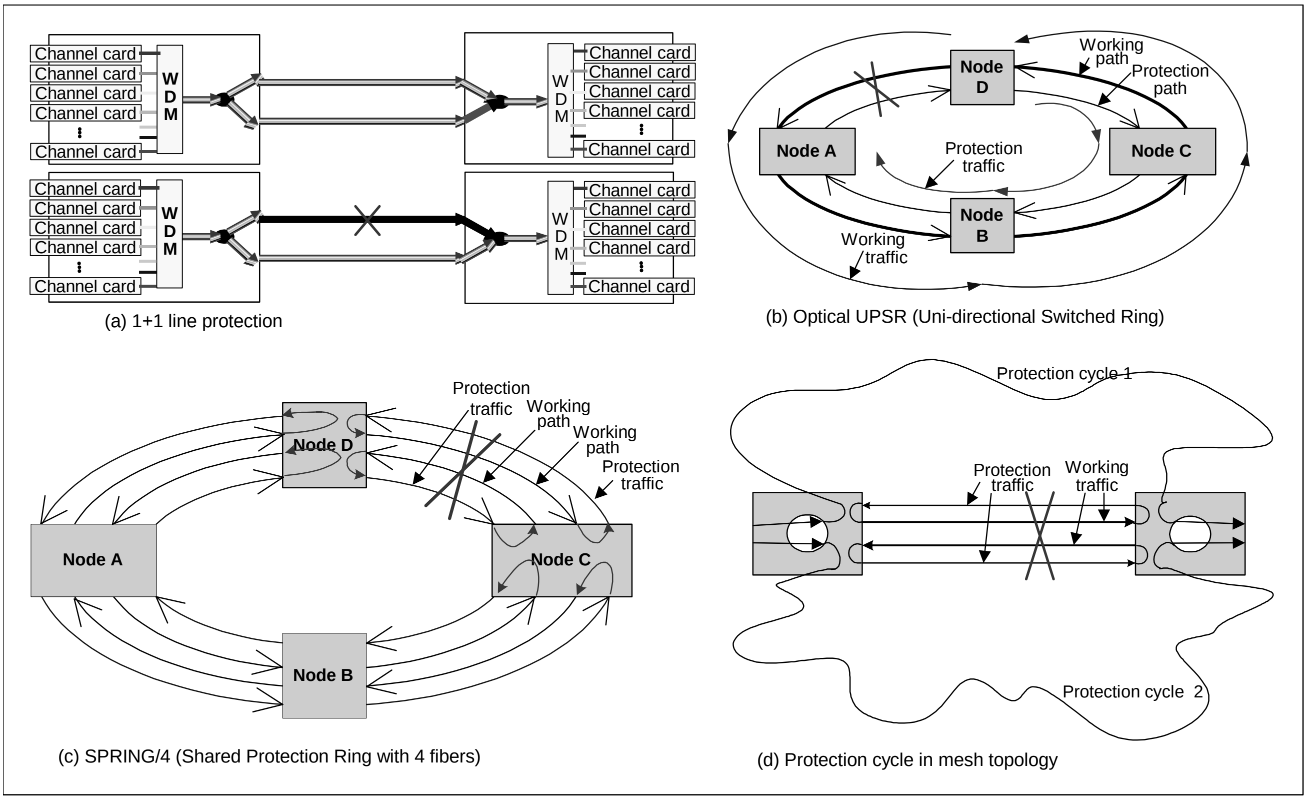


Fig. 1. Restoration (Protection) in the optical layer.

sists of two fibers with working wavelengths and protection wavelengths imbedded in each fiber.

Restoration in a mesh network is shown in Fig. 1(d) where the backup path is planned according to an idea taken from the ring topology; this idea aims to protect one link and is called the protection cycle. The link failure of Fig. 1(d) is restored using a pre-planned protection cycle. Thus, how the protection cycle is calculated has great impact on network restoration performance [16], [17].

2. MPLS Restorations

We review MPLS restoration because our proposed OBS restoration is based mainly on the concept of MPLS restoration.

MPLS restoration generally consists of three steps: fault detection, in which a fault in the network is recognized; fault notification, in which the specific LSR (Label Switching Router) must be indicated by the fault-detecting LSR; and restoration switching, in which the LSR indicated by the fault notification switches traffic from a working path to a protection path (a backup path). The most common method of fault detection is to use a link probing mechanism between neighbor LSRs. One example of a probing mechanism is the periodical exchange of a liveness message between peer LSRs; that is the MPLS-based fault-detection mechanism.

Figure 2 shows the composition of the MPLS protection domain, which is configured to protect one working path. This configuration will be used later in the OBS restoration. The two LSRs at the two points where the working path and backup path meet each other are called Path Switch LSR (PSL) and Path Merge LSR (PML), respectively. The Reverse Notification Tree (RNT) is the same physical path as the working path but it goes in the opposite direction [12], [13].

Restoration in MPLS can be classified into several categories. According to the time when the backup path is calculated and established, there is dynamic rerouting (recovery) and protection switching. Protection switching is faster. According to the range of the working path to be restored, there is global restoration and local restoration. Local restoration has the advantage of fault localization but cannot restore multiple simultaneous faults or a node failure. According to the relationship between a working path and a backup path, there is 1:1(1:N) path mapping and 1+1 path mapping. While in 1:1 path mapping, working traffic is switched to the backup path only after a fault occurs, in 1+1 path mapping the same traffic is transmitted to both the working and backup paths at the same time. When a network failure occurs, the PML simply selects the traffic from the backup path in the 1+1 path mapping.

In normal operation, the resource of a backup path can be shared by extra traffic or be dedicated to working traffic; these are called "extra-traffic allowed" and "dedicated-resource." The indication method can be implemented either using certain control messages, which is called "message-based indication," or by reversing the working traffic to the PSL. These classifications are summarized in Table 1 [12], [20].

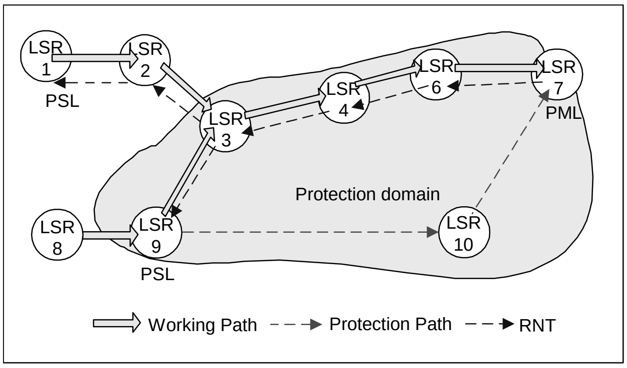


Fig. 2. The MPLS protection domain.

Table 1. Classification of MPLS restoration.

Restoration model	Dynamic rerouting	Protection switching
Scope of recovery	Local restoration	Global restoration
Path mapping	1:1 (1:N)	1+1
Protection path resource	Dedicated-resource	Extra-traffic allowed
Failure notification	Message based	By reversed traffic

Generally, the MPLS restoration procedure is as follows:

① Every node along the working path monitors the network status and detects the occurrence of any type of fault. (Error detection)

② The LSR that detects a fault generates a fault indication message (FIS) and transmits it along the RNT till it reaches the PSL.

③ Each intermediate LSR relays the FIS to the upstream LSR till it reaches the PSL.

④ After receiving the FIS, the PSL realizes the fault in the working path (LSP). If there is the backup path corresponding to the working path, the PSL switches all working traffic on the working path to the backup path.

⑤ If the QoS-routing information about the current topology and resource usage is available, calculate the appropriate path based on that information, and bind the labels along the calculated path by sending a label-mapping message downstream. If necessary, the resource along the path may be reserved. In order to calculate the optimal path, update

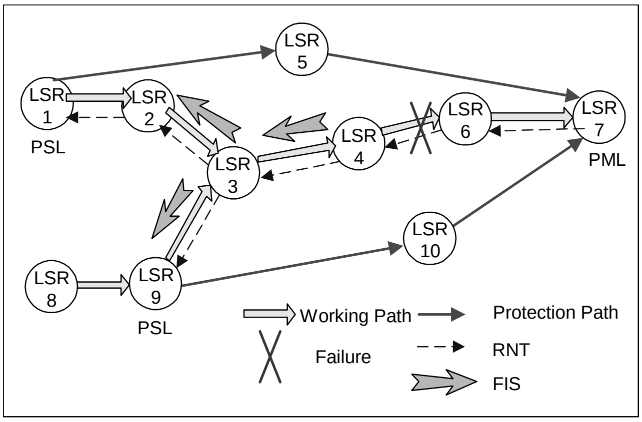


Fig. 3. The MPLS restoration procedure.

the QoS-routing information periodically [12], [14], [18], [21].

III. THE RESTORATION BASED ON OBS

1. Overview of the OBS

From the OBS viewpoint, the optical Internet can be seen as a network internetworking different network domains such as the OBS domain and the non-OBS domain as shown in Fig. 4. The nodes in the OBS domain understand and follow the node operations specified by OBS protocols (which will be briefly explained later) while the node in the non-OBS domain, which includes the MPLS domain, MPλS domain, or other optical network domains, does not have any knowledge of the OBS operations. In order for the OBS domain to internetwork with the non-OBS domain, the edge router in the OBS domain should take care of the appropriate interface work for a seamless transition so that the transportation continues in the OBS domain [1], [4].

An OBS domain consists of edge routers and core routers. When the incoming traffic arrives, the edge router classifies traffic into a corresponding class according to the network management policy and then assembles packets in the same class queue into a proper size data burst. Then the appropriate offset time is determined according to the number of hops to go and the required QoS. A burst control packet (BCP) is generated for a corresponding data burst and sent separately an offset time earlier than the corresponding data burst [4], [22].

In the core router, when the BCP arrives, it is converted into an electric signal for processing. The switching fabric within the core router is configured according to the information from the BCP before the corresponding data burst arrives. Thus, after the offset time, the data burst can pass through the pre-configured optical switch transparently without any O/E/O conversion [4], [22].

Figure 5 illustrates the data burst transmission using the offset time in the OBS domain where node 'Src' and 'Dst' correspond to the edge nodes. 'Src' classifies the packets having the same destination address (the same egress node in the OBS domain) into the same class and assembles them into a properly long burst. The offset time is obtained by considering the delays at each hop, which includes the processing delay for the BCP and the configuration delay of optical components. Thus, the offset time can be expressed as (1) [11].

$$T \geq delay1 + delay2 + delay3 + delay4 \qquad (1)$$

As the BCP proceeds to 'Dst,' its offset time value is updated at each node by subtracting the delay at the current node from the offset time.

Another feature of the OBS is the delayed reservation where a reservation of network resources is made for the time from when the data burst arrives to the time when transmission of the data burst ends. The utilization of network resources can be very efficient with the smart resource management achieved by the delayed reservation.

For efficient network management over the optical Internet,

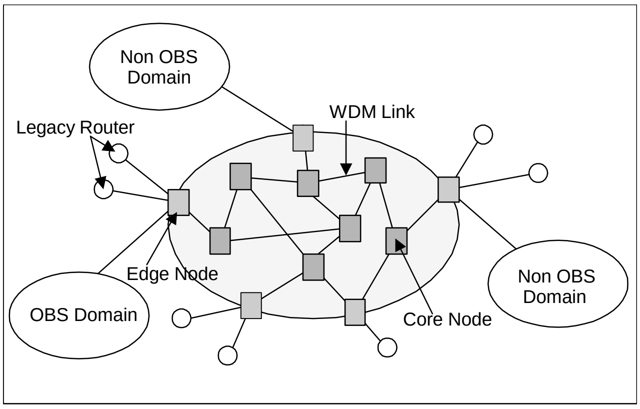


Fig. 4. The OBS network model.

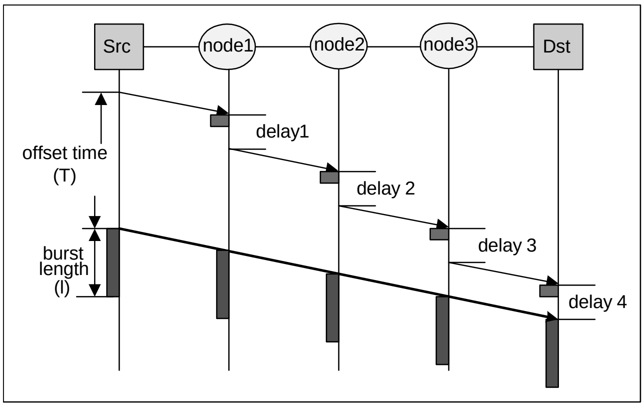


Fig. 5. The concept of OBS.

the control plane issue has to be considered in the OBS domain. Each node in the OBS domain runs the MPLS control plane, which manages network resources through traffic engineering. The control plane takes charge of establishing a label switched path (LSP), which we will call a "virtual LSP" hereafter [11], [23]. To set up the "virtual LSP," each node collects routing information such as network topology and resource usage, and updates the routing table with a QoS routing algorithm [24]. A "virtual LSP" can be established by assigning labels based on this route information where a resource reservation protocol-traffic engineering (RSVP-TE) or constraint-based routing-label distribution protocol (CR-LDP) signaling protocol may be used [25]-[27]. Note that each label within the "virtual LSP" should be mapped into the wavelength available in each node for transporting the data bursts [25], [26] as shown in Fig. 6(b). The details of this architecture were introduced in [11], where the MPLS-control plane-based OBS is called a 'labeled OBS' (LOBS).

A "virtual LSP" in an OBS domain can achieve a much higher efficiency than the one in a GMPLS domain (or a MPλS domain) [11]. In a GMPLS domain (lambda switch) [8], [23], the goal is to reduce the time taken to reconfigure optical paths from months to minutes. Once established as shown in Fig. 6(a), the wavelengths in a lightpath will remain in place for a relatively long time (a session holding time), perhaps months or even years. They can be reconfigured if the lightpath becomes inefficient. In an OBS domain, the goal is to set up a "virtual LSP" by binding a label with a local wavelength at each node (Fig. 6(b)) [8], [23]. The benefits are very clear. By holding the "virtual LSP" only for the duration of the burst, we achieve a statistical multiplexing of the wavelength in the time domain, which can increase the efficiency of network utilization dramatically. In this sense, a "virtual LSP" can be utilized efficiently, and wavelength assignment and traffic engineering problems can be much easier in the OBS domain.

Note that the offset time mentioned above plays an important role in OBS restoration. Since the BCP arrives at the node earlier than the data burst, it is possible to detect a network failure early and respond quickly. In addition, it is very easy to localize a network failure, which makes the restoration quick and transparent to other nodes.

2. Network Failures and Detections

In the optical Internet, a link between two nodes is composed of several optical fibers, each of which carries many wavelengths (or channels). The channels are divided into the control channel group (CCG) for the transmission of control messages and the data channel group (DCG) for the transmission of data bursts [22]. Thus, several types of optical network faults can exist depending on the location of the fault: data channel failure, control channel failure, fiber failure, link failure, and node failure. Figure 7 shows the different types of failure in the optical Internet.

When a network fault occurs, it is desirable that the restoration should be done as soon as possible. The restoration time is highly dependent on the fault detection time. The detection mechanisms in the higher layer, such as the MPLS-based fault-detection mechanism [12], take a relatively long time to detect a fault. Hence, it is necessary to adopt a fault detection mechanism in the optical layer, which can detect the fault faster.

First, it is possible to detect the channel failure by monitoring the optical signal quality per wavelength. It is important to

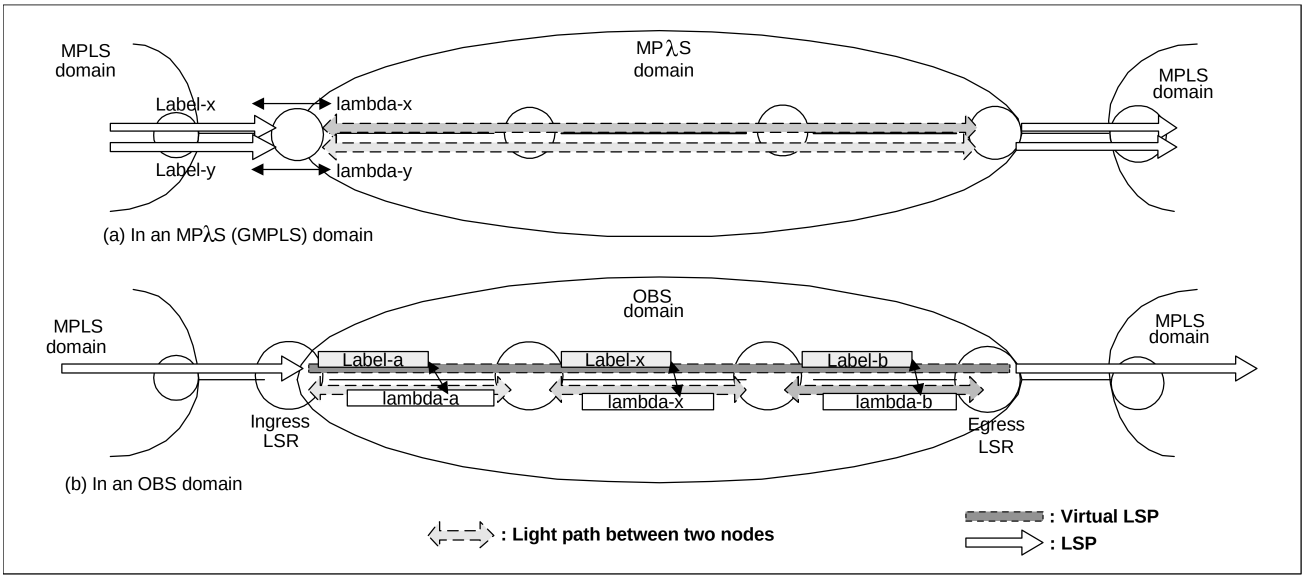


Fig. 6. A binding LSP with wavelength in MPλS and OBS domains.

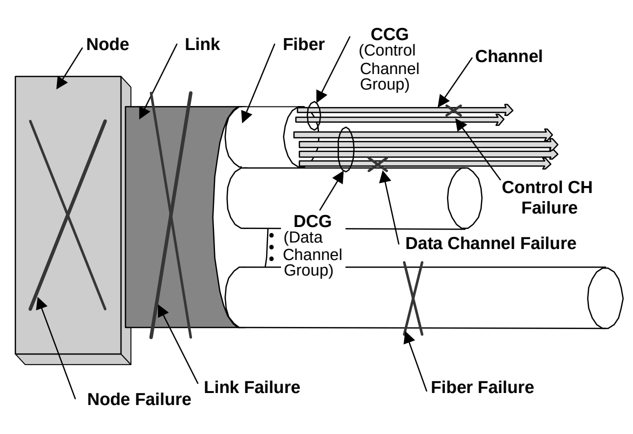


Fig. 7. Types of network failure.

manage the states of all channels, and in order to recognize the specific fault, the control channel and its corresponding data channel must be managed as a pair. Second, it is possible to detect the fiber failure by applying the state information per fiber by monitoring the loss of light (LOL) as shown in Fig. 8. When the state changes from 'ACTIVE' to 'DISCONNECT' by detecting an LOL, a fiber failure is made. Third, the detection of a link failure is implicitly determined by using the state of fibers belonging to this link. In other words, when the states of all fibers within a link change into DISCONNECT, it is assumed to be a link failure. Finally, the detection of a node failure is made by checking two conditions as follows. Every node exchanges liveness messages with its neighbor nodes and counts the number of the messages periodically to check its normality. When the number of liveness messages is zero at the checking time, it is assumed to be a semi-node failure, and then the states of the corresponding control channel and fiber must be checked to decide whether the semi-node failure has resulted from a control channel failure. If the states of the channel and the fiber are normal, it is determined to be a node failure.

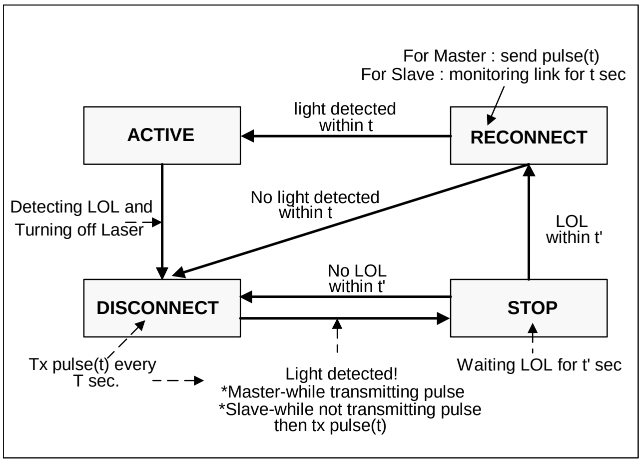


Fig. 8. The state diagram of OFC (Open Fiber Control) [16].

3. The Restoration Procedure in the OBS Domain

We classify OBS-based restoration as link-level restoration or path-level restoration. The link-level restoration is done at the local node, while the path-level restoration is done globally between the OBS PSL (OPSL) and OBS PML (OPML). For path-level restoration, the OPSL and OPML must be equipped with intelligent functions and an alternative "virtual LSP" because restoration must be pre-established for each working "virtual LSP." In addition, the path for the indication message should be established in advance, and this path is called the OBS Reverse Notification Tree (ORNT) [12], [23]. These configuration concepts are similar to those of MPLS introduced in the previous section. For the link-level restoration, we configure each link in a way that each instance within a link has a corresponding backup instance; thus, there are working fibers with backup fibers and working channels with backup channels to achieve the 1:N restoration scheme.

The objective of OBS restoration is to maximize the fault localization, which results in faster restoration and better utilization. Thus, link-level restoration is tried as a first step if possible. If it fails, path-level restoration is tried. If it fails again, an alternative backup path (for path-level restoration) is dynamically calculated for the restoration. If all above methods fail, the network capacity must be re-planned and provisioned for proper survivability [18], [28].

The OBS restoration procedure can be explained in detail as follows. Every node in the OBS domain monitors the network status using the fault detection mechanism introduced previously. When a fault is detected, the appropriate restoration scheme is triggered as shown in Fig. 9. For a channel failure or fiber failure, link-level restoration will be tried, while for link failure and node failure, the path-level restoration will be tried. Note that for the link failure, if the traffic has a high priority, the "Bossy LSR" is applied; this will be described later.

For a channel failure, the data channel and control channel must be considered together. If a fault occurs in either a control or a data channel and the corresponding backup channel is available, 1:N restoration can successfully be completed. Fig. 10(a) shows the link-level restoration procedure when the control channel has a fault. Node-b, which detected the channel failure, replaces the control channel affected by this fault with the backup channel. This node updates the content of BCP-2 received from node-a and activates the backup channel by transmitting it. In this way, the data forwarding channel will hardly be affected by the channel failure.

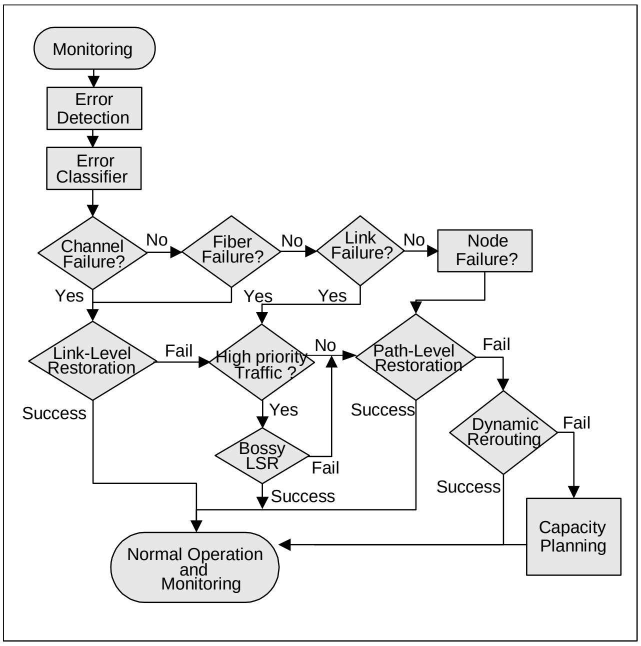


Fig. 9. The procedure for OBS restoration.

In Fig. 10(b), link level restoration is executed in order to restore a data channel failure. In this case, the data burst affected by the data channel failure (e.g., burst-2) has to be addressed in some way. This affected traffic is defined as "link-level unrestored" traffic, which will be explained later.

When both the control and the data channels have failures at the same time, link-level restoration is applied first. If these two channels, acting as a pair, cannot be restored using link-level restoration, path-level restoration will be tried. Fig. 10(c) explains the path-level restoration where node-b in Fig. 9(c) can restore the data channel but it does not have an available backup control channel. Then, node-b sends the FIS upstream along the control channel to the OPSL as soon as it detects a fault. After receiving the FIS, the OPSL starts to switch all traffic on the working path to the backup path. This backup path will be activated by the first arriving BCP (e.g., BCP-3 in Fig. 10(c) transmitted along this backup "virtual LSP"). Note that while the FIS is being transferred to the OPSL, the data burst and control packet existing on the affected working path can be lost, which is called "path-level unrestored" traffic. Restoration

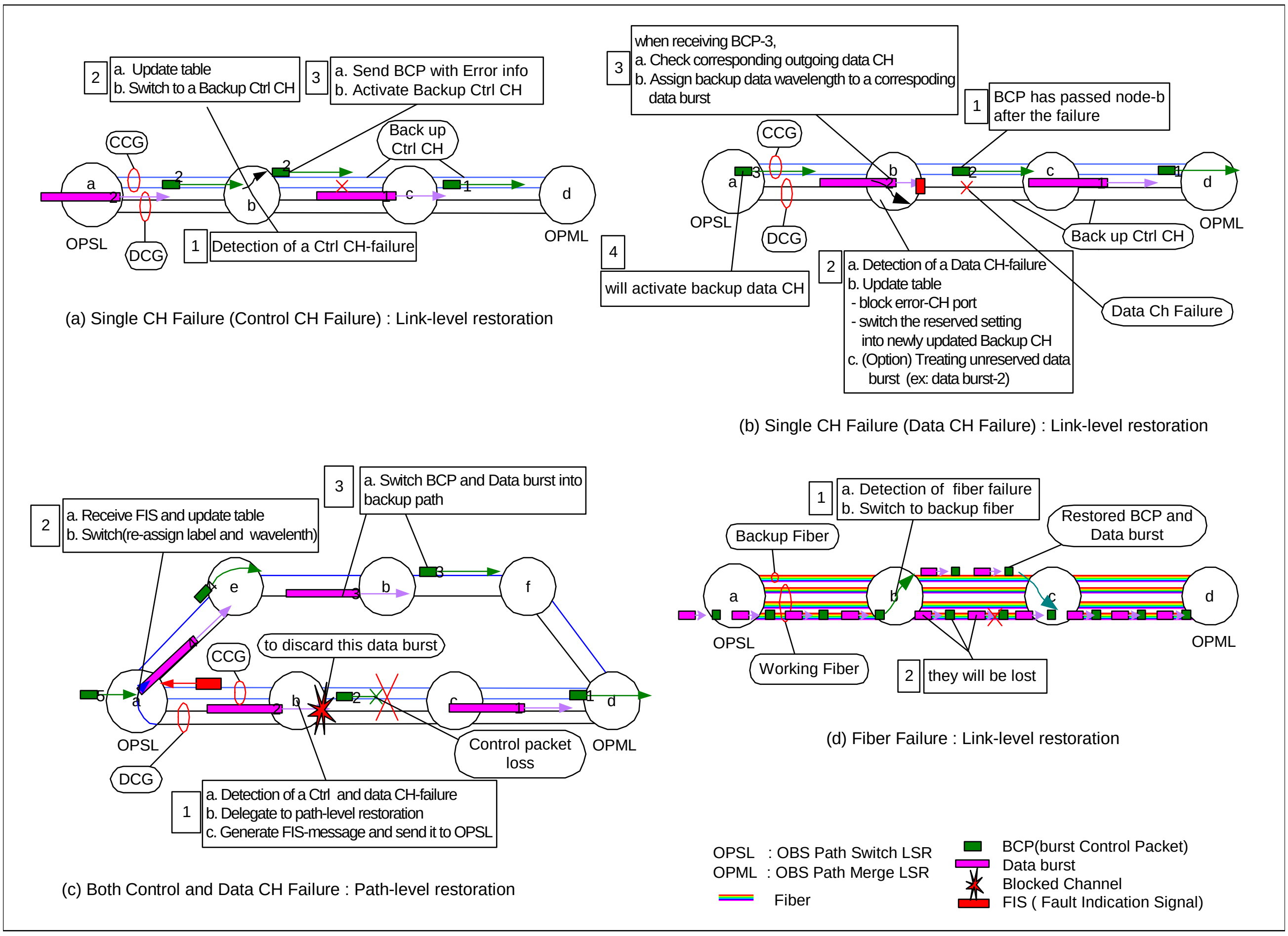


Fig. 10. Restoration procedures for various failure types.

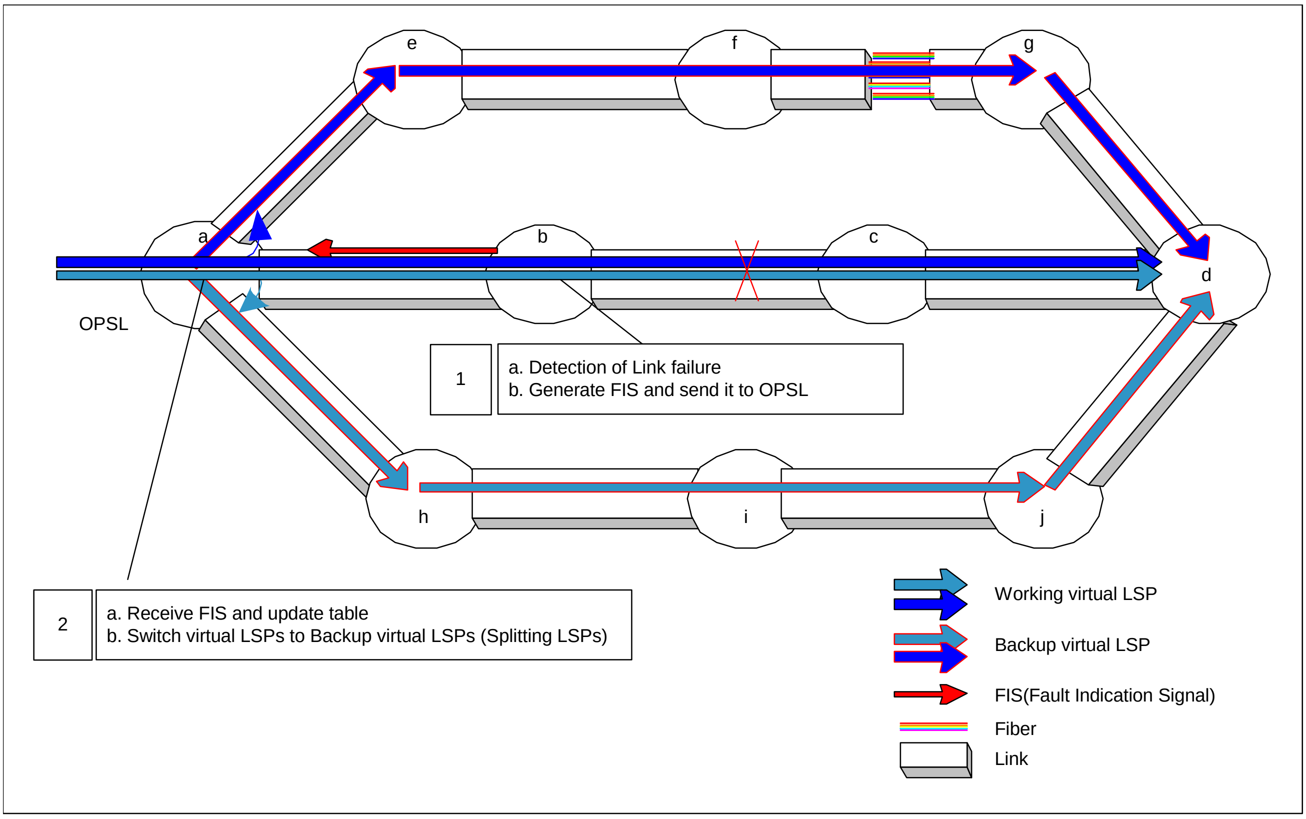


Fig. 11. Link failure and its restoration procedure.

of "path-level unrestored" traffic will be explained later.

For a fiber fault, the link-level restoration is executed. Figure 10(d) illustrates how all the traffic on the working fiber is switched into the backup fiber. But if the backup fiber is already occupied or has a fault at the same time as the working fiber, it triggers the path-level restoration immediately. We call this restoration method with unrestored traffic 'simple path-level restoration' from now on.

For a link or node failure, path-level restoration applies directly. A link or node failure can cause a huge number of "virtual LSPs" (large volume of traffic) to be restored. Thus, as shown in Fig. 11, the OPSL may split the restored traffic into several backup paths, which must be pre-planned [23].

If all the methods mentioned above fail, the backup path will be dynamically calculated based on the collected routing information, which is dynamic rerouting. If the dynamic rerouting fails, the network capacity must be re-planned to ensure survivability [18].

4. Special Cases and Semi-Fault Localization

This section describes the special cases that might be caused by OBS restoration: unrestored traffic, unnecessary reservation, and semi-fault localization using the "bossy LSP."

A. Treating Unrestored Traffic

There are two types of unrestored traffic: "link-level unrestored" traffic and "path-level unrestored" traffic. When a channel or fiber failure occurs, some BCPs may have already passed the node (e.g., in Fig. 10(b) node-b) and the corresponding data bursts will be lost. We call this "link-level unrestored" traffic (e.g., in Fig. 10(b) data burst-2 will be lost). In addition, data bursts arriving before the path-level restoration begins (until the OPSL receives the FIS) will be lost. We call this "path-level unrestored" traffic. In other words, they are being transferred on the fault-affected "virtual LSP" while this FIS is being transferred to this OPSL, as shown in Fig. 12(a). Note that this is the original problem of MPLS restoration.

The restoration of the unrestored traffic depends on the service level required by the traffic. If the traffic requires only the best-effort service, the node having the (link-level or path-level) unrestored traffic simply discards it, which reduces the complexity of the system.

If the unrestored traffic requires a low loss rate, "link-level unrestored" and "path-level unrestored" traffic has to be restored. In order to restore "link-level unrestored" traffic, the node detecting the channel or fiber failure generates a newly

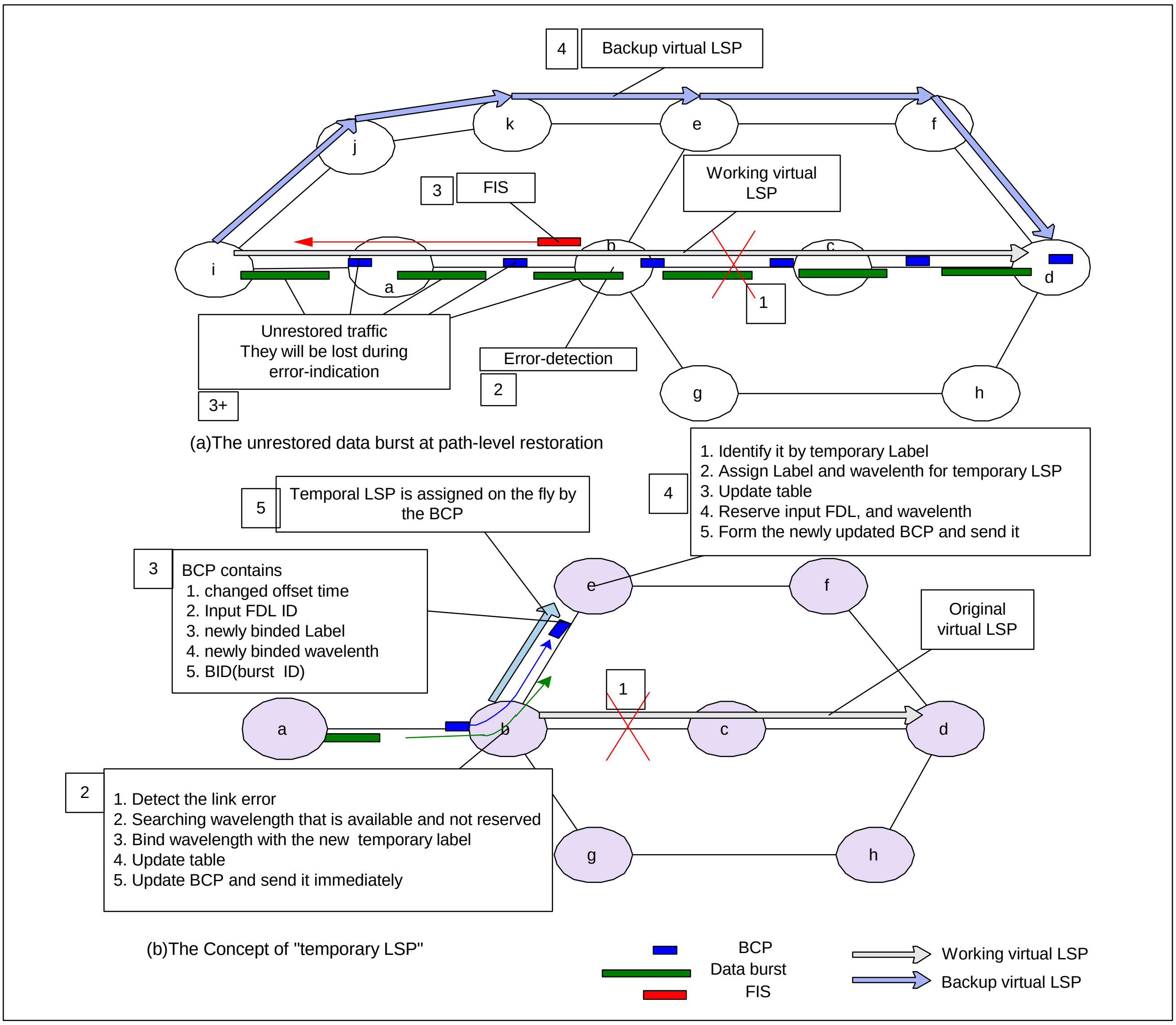


Fig. 12. Unrestored traffic.

updated BCP, which contains a new offset time, the newly mapped label, the wavelength, and the failure information, and immediately sends it along the control channel (e.g., in Fig. 10(b) a new BCP-2 will be generated again). Of course, the corresponding data bursts must be delayed through a fiber delay line (FDL) to compensate for the time spent on generating the new BCP plus the difference between the original offset-time and the offset-time for the new route. The nodes on the downstream path recognize the occurrence of the data channel failure by receiving the BCP and make a new reservation.

In order to restore "path-level unrestored" traffic, restoring "path-level unrestored" traffic takes advantage of the newly proposed "temporary LSP" method, which is illustrated in Fig. 12(b). The "temporary LSP" is another backup path, which is a shortcut from the fault-detecting node to an OPML for the temporary purpose of restoring "path-level unrestored" traffic. Until the local node (e.g., node-b in Fig. 12) completes the path-level restoration after sending the FIS to the OPSL, the "temporary LSP" is used to restore "path-level unrestored" traffic arriving at the local node during that period. The "temporary LSP" will be released after "path-level unrestored" traffic is restored. To implement the "temporary LSP," each node needs to reserve a small portion of label space, which will be used when establishing the "temporary LSP" on the fly, and maintain the shortcut path information, keeping it up-to-date. Thus, this scheme can reduce the loss rate and restoration time. As soon as the local node detecting the fault sends the FIS to the OPSL, it generates a BCP with a temporary label selected from the reserved label space with one of the available wavelengths and sends it to the pre-planned path. A "temporary LSP" can be established along the downstream nodes by assigning a label in the reserved label space [26] and is mapped with locally available wavelengths, which is similar to the 'suggested label' of the Generalized MPLS [29]. From now on we call this method "path-level restoration with temporary LSP" or just "temporary LSP" for simplicity.

B. Unnecessary Resource Reservation

When any type of fault occurs just after the BCP has passed the node, this BCP will make an unnecessary reservation of the resource at the downstream nodes. This causes other traffic to be blocked at the downstream nodes (Fig. 13(a)). To ease this problem, the unnecessary reservation should be released as shown in Fig. 13(b). As each node receives the BCP, it sets a timer and waits for 'offset time + alpha' until it receives the corresponding data burst. If this data burst arrives within that period, the node resets the timer. Otherwise, the unnecessary reservation is assumed, and the reserved resources are released immediately.

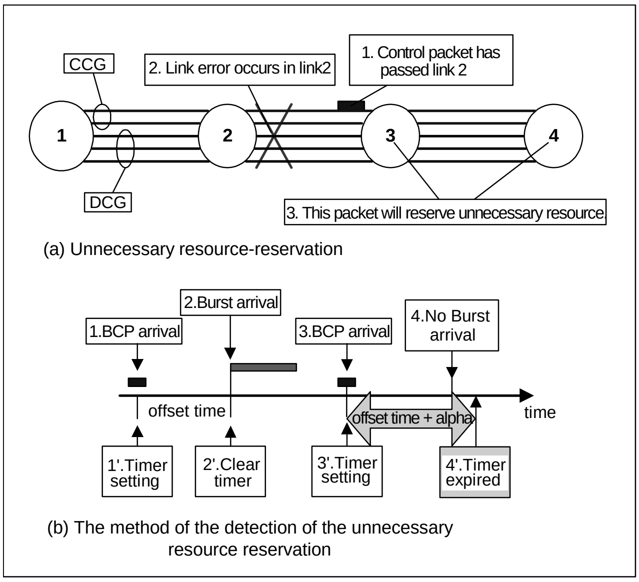


Fig. 13. The unnecessary reservation.

C. Bossy LSP

When link-level restoration fails or link failure occurs, path level restoration is applied. Normally, path-level restoration requires the local node detecting the fault to send an FIS to the OPSL, and OPSL to initiate the restoration; this results in a comparatively low utilization and a long restoration time. Thus, if the traffic needs to be restored fast, simple path-level restoration is inappropriate. In order to provide fast service, we propose the "bossy LSP." Conceptually, the "bossy LSP" is the same as the "temporary LSP"; however, it is different from the "temporary LSP" in that the latter releases the LSP after "path-level unrestored" traffic is restored, while the former establishes the LSP as a permanent use. In addition, the "bossy LSP" allows the preemption attribute in the BCP fields so that when the "bossy LPS" reserves the label (and wavelength), it can preempt the lower priority LSP. However, if all resources are occupied by other "bossy LSPs," then simple path-level restoration will be tried. We call this method "path-level restoration using bossy LSP," or simply a "bossy LSP." A "bossy LSP" could also be called "semi-fault localization" because the restoration covers the path from the local node detecting the fault to the OPML.

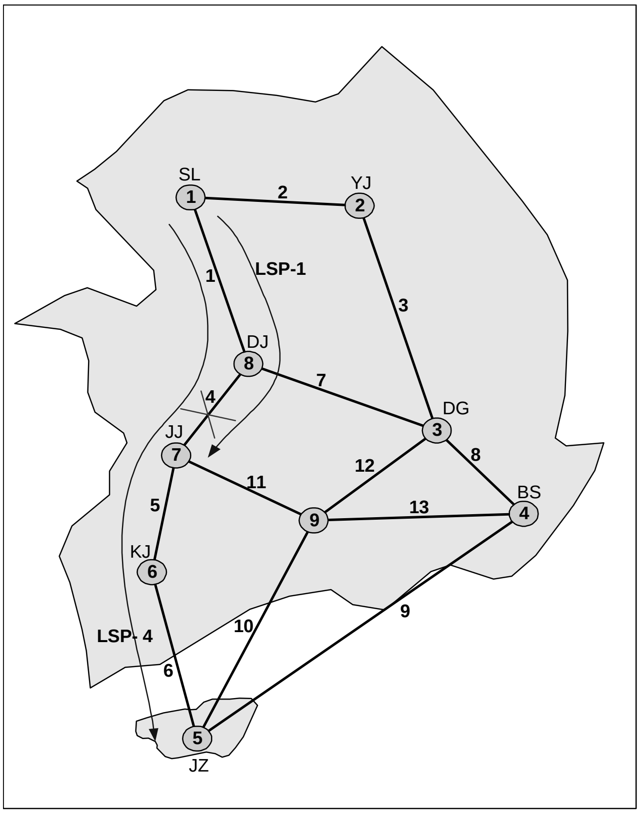


Fig. 14. The network topology for simulation.

IV. SIMULATION AND RESULTS

1. Simulation Model

In this section, we present the simulation results of the OBS restoration. For the simulation we consider the network topology as shown in Fig. 14, where the OBS domain consists of 9 nodes. Note that any node can be either an ingress node or an egress node, and the multiple "virtual LSPs" interconnect the nodes. In the simulation we configure 6 "virtual LSPs." In order to effectively show the restoration results, we generate the traffic into each LSP with a continuous data burst stream with a constant bit rate. We consider three types of network failure: channel failure, fiber failure, and link failure. Since the restoration time for both channel and fiber failures is too fast to distinguish, we only focus on the case of the link failure. For comparison purposes, the path-level restoration for the link failure is done using three methods: (1) simple path-level restoration, (2) "temporary LSP," and (3) "bossy LSP." The simulation results are obtained when link 4 in Fig. 14 has a link failure.

2. Simulation Results

We plotted the simulation results by measuring the amount of traffic received at the destined egress node as well as the restoration time. In Fig. 15 through Fig. 17, the X and Y axes represent the time in microseconds and the data rate in bits per second, respectively.

Figure 15 shows the amount of loss incurred and the restoration time in virtual LSP 4. The restoration time of the LSP is about 7.3 ms. The amount of traffic loss is quite huge compared to the other two graphs (Figs. 16 and 17). The following three factors explain the loss: the loss during fault detection, the loss of "link-level unrestored" traffic, and the loss of "path-level unrestored" traffic.

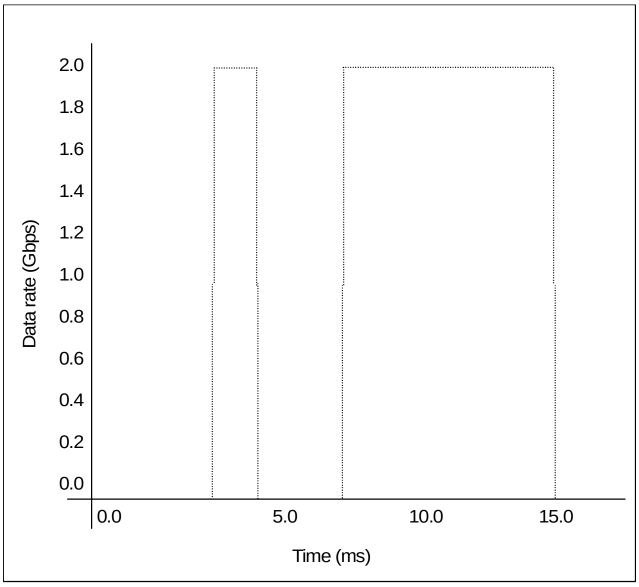


Fig. 15. Simple path-level restoration.

Table 2. Loss rate and restoration time.

	Simple path-level restoration	"Temporary LSP"	"Bossy LSP"
	LSP-4	LSP-4	LSP-4
Loss rate (%)	18.77	5.24	5.06
Restoration time (ms)	7.3	5.3	5.3

The restoration time in Figs. 16 and 17 is significantly less (about 5.3 msec restoration time for virtual LSP 4) than that in Fig. 15. For restoration time, the "temporary LSP" is as fast as the "bossy LSP." In addition, as compared to Fig. 15, the loss is dramatically reduced by eliminating the loss of the "path-level unrestored" traffic. Table 2 summarizes these loss rates and restoration times.

In particular, a comparison of Fig. 16 ("temporary LSP") with Fig. 17 ("bossy LSP") shows that the "bossy LSP" gives a continuous data delivery service, while the "temporary LSP" gives an interruption in data delivery. The interruption in the

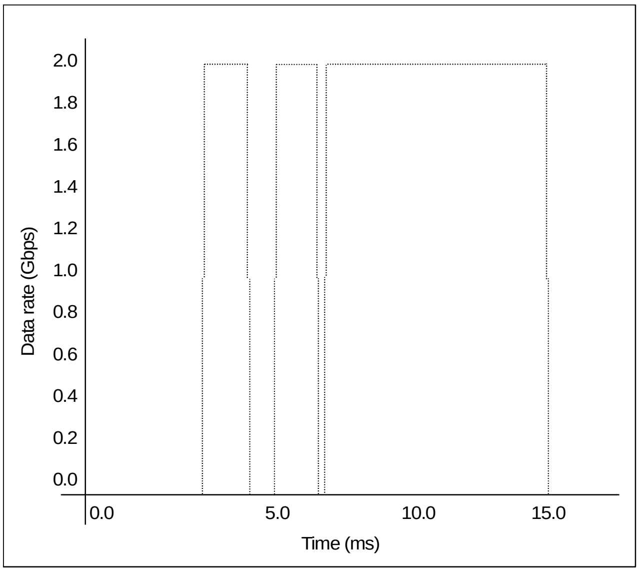


Fig. 16. Temporary LSP.

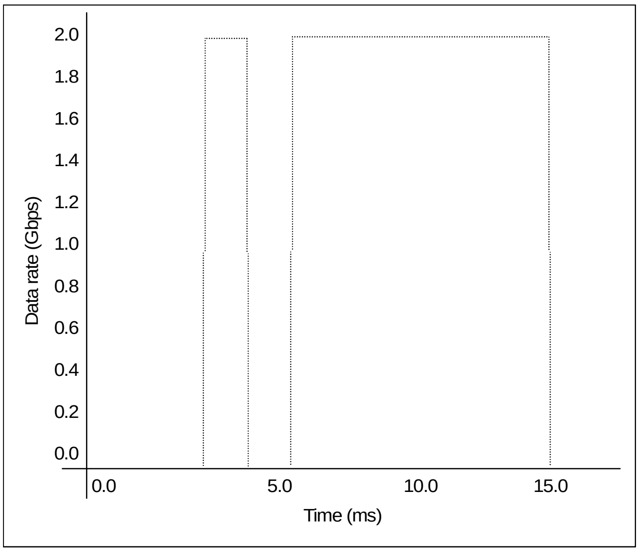


Fig. 17. Bossy LSP.

"temporary LSP" can be explained by the fact that while the "path-level unrestored" traffic is restored immediately using the "temporary LSP," the restoration at the OPSL takes some time (restoration delay) due to the comparatively long backup route, which is shown in Fig. 16 as the second valley. The simulation results demonstrate that the "bossy LSP" outperforms the other two restoration methods.

V. CONCLUSION

As the optical Internet has become accepted as the infrastructure for the next generation Internet, the issue of survivability has become more and more important. In particular, the optical burst switching technique has been gaining power as the one of the feasible candidates for the optical Internet, so it is now an urgent matter to address the survivability issue.

As background for our study, we comprehensively reviewed the existing protection/restoration schemes for both optical networks and IP (MPLS) networks and identified the key features of the OBS. Then, to provide seamless connectivity between the OBS domain and non-OBS domain, we clarified the internetworking of those two domains. Further, we explained in detail a fault detection technique for all kinds of faults that might occur in the optical Internet. We fully discussed the proposed OBS restoration procedures as well as the concept of the "temporary LSP" and "bossy LSP." We demonstrated that OBS restoration can survive various types of network failure and achieve a fast restoration with high network utilization. We also showed that the "temporary LSP" and "bossy LSP" can enhance the fault localization for fast restoration and dramatically reduce loss as well. Furthermore, the "bossy LSP" is better than the "temporary LSP" in the aspect of bandwidth utilization and service continuity. We conclude that the proposed OBS restoration effectively restores all types of network failure and provides a good survivability in the optical Internet. There is a need for further studies in OBS restoration, specifically, it is necessary to develop an OBS-specific routing algorithm for OBS restoration which meets the following requirements:

- Calculation of a working path with a backup path that can accommodate the maximum number of the future connections.
- Traffic engineering that can resolve channel contention problems (the FDL limitation) and result in the better network utilization.

REFERENCES

[1] M. Yoo and C. Qiao, "Just-enough-time (JET): A High Speed Protocol for Bursty Traffic in Optical Networks," *Dig. Of IEEE/LEOS Summer Topical Mtgs. Technologies for a Global Info. Infrastructure*, Aug. 1997, pp. 26-27.

[2] Byoung Seung Ham, "A Novel Method of All-Optical Switching: Quantum Router," *ETRI J.*, vol. 23, no. 3, Sept. 2001, pp. 106-110.

[3] S.H. Song and E.H. Lee, "3-Dimensionally Integrated Planar Optics for 100 Gb/s Optical Packet Address Detection," *ETRI J.*, vol. 17, no. 2, July 1995, pp. 1-10.

[4] C. Qiao and M. Yoo, "Optical Burst Switching (OBS): A New Paradigm for and Optical Internet," *J. High Speed Networks, Special Issue on Optical Networking*, vol. 8, no. 1, Jan. 1999, pp. 69-84.

[5] Tai Won Um et al., "Signaling and Control Procedures using Generalized MPLS Protocol for IP over Optical Network," *ETRI J.*, vol. 24, no. 2, Apr. 2002, pp. 69-80.

[6] M. Yoo et al., "Optical Burst Switching for Service Differentiation in the Next-Generation Optical Internet," *IEEE Comm. Mag.*, Feb. 2001, pp. 98-104.

[7] G. Mohan et al., "Lightpath Restoration in WDM Optical Networks," *IEEE Network*, Nov. 2000, pp. 24-32.

[8] Ayan Banerjee et al., "Generalized Multi-protocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques," *IEEE Comm. Mag.*, July 2001, pp. 144-151.

[9] Ayan Banerjee et al., "Generalized Multi-Protocol Label Switching: An Overview of Routing and Management Enhancements," *IEEE Comm. Mag.*, Jan. 2000, pp. 144-150.

[10] Murali Kordialam et al., "Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks," *IEEE INFOCOM 2001*, pp. 358-366.

[11] Chunming Qiao, "Labeled Optical Burst Switching for IP-over-WDM Integration," *IEEE Comm. Mag.*, Sept. 2000, pp. 104-114.

[12] Vishal Sharma et al., "Framework for MPLS-based Recovery," Internet draft, draft-ietf-mpls-recovery-frmwrk-03.txt, July 2001.

[13] Thomas M. Chen and Tae H. Oh, "Reliable Service in MPLS," *IEEE Comm. Mag.*, Dec. 1999, pp. 58-62.

[14] Robert Doverspike et al., "Challenges for MPLS in Optical Network Restoration," *IEEE Comm. Mag.*, Feb. 2001, pp. 89-96.

[15] Yinghua Ye et al., "On Joint Protection/Restoration in IP-Centric DWDM-Based Optical Transport Networks," *IEEE Comm. Mag.*, June 2000, pp.174-183.

[16] Rajiv Ramaswami and K. N. Sivarajan, *Optical Networks: A Practice Perspective*, Morgan Kaufmann Publishers, 1998.

[17] A. Fumagalli and L. Valcarenghi, "IP Restoration vs. WDM Protection: Is There an Optimal Choice?," *IEEE Network*, Nov/Dec. 2000, pp. 34-41.

[18] Gerald R. Ash, "Traffic Engineering & QoS Methods for IP-,ATM-,&TDM-Based Multiservice Networks," Internet draft, draft-ietf-tewg-qos-routing-01.txt, Mar. 2001.

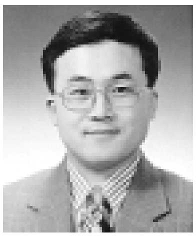
[19] Ornan Gerstel et al., "Optical Layer Survivability – An Implementation Perspective," *IEEE J. Select. Areas Comm.*, vol. 18, no. 10, Oct. 2000, pp.1885-1899.

[20] Dimitry Haskin et al., "A Method for setting an Alternative Label Switched Paths to handle Fast Reroute," Internet draft, draft-haskin-mpls-fast-reroute-05.txt, Nov. 2000.

[21] Anwar Elwalid et al., "MATE: MPLS Adaptive Traffic Engineering," *IEEE INFOCOM 2001*, pp. 1300-1309.

[22] Yijun Xiong et al., "Control Architecture in Optical Burst-Switched WDM Networks," *IEEE J. Select. Areas Comm*., vol. 18, no. 10, Oct. 2000, pp.1838-1851.
[23] D. Awduche et al., "Multi-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control With Optical Cross-Connects," Internet draft, draft-awduche-mpls-te-optical-03.txt, Nov. 1999.
[24] Shigang Chen and Klara Nahrstedt, "An Overview of Quality of Service Routing for Next-Generation High-Speed Networks: Problems and Solutions," *IEEE Network*, Nov/Dec. 1998, pp. 64-79.
[25] P. Ashwood-Smith et al., "Generalized MPLS Signaling-CR-LDP Extensions," Internet draft, draft-mpls-generalized-cr-ldp-02.txt, Apr. 2001.
[26] P. Ashwood-Smith et al., "Generalized MPLS-Signaling Functional Description,“ Internet draft, draft-ietf-mpls-generalized-signaling-03.txt, Apr.2001.
[27] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switched Architecture," IETF RFC 3031.
[28] Jong Hyup Lee, "Design and Configuration of Reconfigurable ATM Network with Unreliable Links," *ETRI J*., vol. 21, no. 4, Dec. 1999, pp. 9-22.
[29] Peter Ashwood-Smith et al., "Generalized MPLS – Signaling Functional Description," Internet draft, draft-ietf-mpls-generalized-signaling-07.txt, Nov. 2001.

Seunghun Oh received BS and MS degrees in electrical engineering from Soongsil University, Seoul, Korea, in 2000 and 2002, respectively. He is currently a PhD student in the School of Electronic Engineering, Soongsil University, Seoul, Korea. His current research interests are Optical Internet including optical burst switching, protection/restoration, DiffServ-aware traffic engineering, and routing issues.



Younghan Kim received his BS degree in electronics engineering from the Seoul National University, Seoul, Korea, in 1984, and MS and PhD degrees in electrical engineering from the Korea Advanced Institute of Science and Technology, Seoul, in 1986 and 1990, respectively. From 1987 to 1994 he was a Senior Member of the research staff in the Digicom Institute of Telemetics, Seoul, Korea. Since September 1994 he has been with Soongsil University, where he is currently an Associate Professor in the School of Electronic Engineering.

Myungsik Yoo received BS and MS degrees in electrical engineering from Korea University, Seoul, Korea, in 1989 and 1991, respectively, and his PhD degree in electrical engineering from State University of New York at Buffalo (SUNY at Buffalo), Buffalo, NY, USA, in 2000. He worked for Nokia Research Center, Burlington, MA, USA, as a Senior Research Engineer. He has been an Assistant Professor in the School of Electronic Engineering, Soongsil University, Seoul, Korea since Sept. 2000. His current research interests are WDM optical networks and Optical Internet including optical burst switching, protection/restoration, QoS support, and control and management issues.

Hyun Ha Hong was born in Yuncheon, Korea, in 1956. He received his BS degree from Kwangwoon University, in 1979, and his MS degree from Yonsei University, Seoul, in 1981, both in electronic engineering. In 1985, he joined Electronics and Telecommunications Research Institute (ETRI). He is now a Team Leader of optical packet router team at optical communication department there. His current research areas of interest include optical packet/burst switched networks for Internet traffic, optical switch architectures, and performance analysis.