# Concurrent Failures and Redundant Protection Problem in Hierarchical GMPLS Networks

Sung-eok Jeon
Department of Electrical and Computer Engineering, Georgia Tech, Atlanta, USA
Email: sejeon@ece.gatech.edu

***Abstract*— The generalized multiprotocol label switching (GMPLS) networks attain a hierarchical structure, and each layer maintains an independent protection mechanism, resulting in redundant protection. The common pool method provides a basic approach to solve the redundant protection problem. Although the common pool method is simple and robust, however it can fail in some cases. This work first shows that none of the prior work satisfies both redundant protection and two links failure problem simultaneously. Moreover, this work also presents a new type of two links failure problem (i.e., the failure of two links at two different layers), which can happen frequently and the common pool method cannot cope with. To solve the proposed two links failure problem, while minimizing the cost of redundant protection problem, this work proposes a new protection scheme for hierarchical GMPLS networks.**

***Index Terms*— GMPLS Networks, Survivability, Spare Network, Common Pool Method, Hamiltonian Cycle.**

## I. INTRODUCTION

The multiprotocol label switching (MPLS) networks play an important role as the transport network of the next generation Internet (NGI). Lots of studies have been proposed for the protection problem at the MPLS networks, and thus important working paths are to be protected by reserved backup paths. Thus, each active connection of MPLS network is usually protected by redundant backup paths [5]. The concept of MPLS is extended to the generalized multiprotocol label switching (GMPLS) by generalizing the concept of MPLS label. The IP/MPLS and optical networks are combined together by using GMPLS networks as the common control plane. Because these two networks (i.e. MPLS and optical) are developed independently, they keep their protection schemes independently, and their protection schemes do not interact with each other. Thus, the multi-layer survivability in the GMPLS networks can cause redundant protection and waste of network resources.

Lots of protection methods are proposed in the literature. For the redundant protection problem in the GMPLS networks, the common pool method is proposed in the literature [5], which is originally proposed to solve the redundant protection problem in the asynchronous transfer mode (ATM) over wavelength division multiplexing (WDM) networks. With the common pool method, a backup path of a layer $i+1$ uses the spare network of the lower layer $i$, which is the collection of backup paths at layer $i$. Now, because the backup paths of the layer $i+1$ use the already reserved spare network of the layer $i$, there is no redundant protection. Thus the common pool method solves the redundant protection problem completely.

However the common pool method can fail in some cases, which may happen so frequently. For example, if there is a link failure at a layer $i$, a part of the spare network of the layer $i$ come to busy due to the working paths using the failed link. Thus, some backup paths of layer $i+1$ are disabled until the failed link of layer $i$ is repaired and the backup paths of layer $i$ becomes idle. The problem is that due to different layer property, $(i)$ a link of layer $i+1$ may fail much frequently than that of layer $i$, and $(ii)$ a failed link of layer $i$ may not be recovered for a long time. This causes the active flows of layer $i+1$ to work without any backup paths, which is called as "concurrent failure of two links at two different layers".

To solve this problem, this work first classifies the relationship between two adjacent layers (e.g. layers $i$ and $i+1$) in the hierarchical networks. That is, if the domain of layer $i$ exactly overlaps with that of layer $i+1$, these two adjacent layers are called "overlapping layers". Otherwise, these two adjacent layers are called "non-overlapping layers". This work shows that the problem of "concurrent failure of two links at two different links" does not exist between overlapping layers. We also show that this problem exists between non-overlapping layers, and can cause the common pool method to fail. Thus, for the overlapping layers, the common pool method can be used. For the non-overlapping layers, however, this work proposes two new methods to solve this problem: method I – use several partial protections instead of an end-to-end protection; method II – use a modified common pool method. The method II is preferred because of its easy applications to the real networks.

The rest of the work is organized as follows. In Section II, this work reviews the previous studies on the connection restoration methods in the core networks and the existing models on the redundant protection problem in the literature. In Section III, this work shows the potential problem of the common pool method. The proposed protection schemes are presented in Section IV, whose performance are compared in Section IV-C. Finally, in Section V, some discussions will conclude the work.

Based on "Redundant Protection Problem in the Hierarchical GMPLS Networks," by S. Jeon which appeared in the Proceedings of the IEEE International Conference on Local Computer Networks (LCN) 2005, Sydney, Australia, November 2005. © 2005 IEEE.

## II. Related Work

### A. Protection and Restoration

To protect a connection failure, there are two feasible approaches [1], [11], [14], i.e., proactive and reactive restoration. The proactive schemes reserve backup paths for a working path in advance, however the reactive schemes only reroute a failed connection onto another feasible route after a failure happens. Each restoration scheme also can be classified into a link- and path-based one.

Each scheme has its own merits and demerits. The reactive method does not waste the network resources because it does not set up any redundant spare networks in advance. However, it can cause a long delay until a connection is recovered. This is because it only starts finding another route after a connection failure happens. The proactive method makes the network react faster at a connection failure by rerouting the traffic onto the pre-reserved backup path. However, this method uses more network resource than the reactive method. The reactive method is now used for the connection recovery in IP layer, and the proactive method is used for the core (optical) networks, in which each network component carries huge amount of network traffic. In IP network, the recovery time is not a big deal. However, in the core networks, the recovery time for a failed link is critical. It is expected for a failed component to recover within few milliseconds.

Depending on the importance of a working path, the backup mechanism can be chosen from $1:1$, $1+1$, or $1:n$ backup. The redundant spare network for backup paths can be used to carry less important traffic (e.g., best-effort traffic) while backup paths are free. When the backup paths are used to reroute active connections, the less important traffic is preempted. This backup scheme is a general concept in the core networks. However, in the hierarchical networks (e.g., MPLS over optical network), where independently developed networks are merged together, the backup scheme causes redundant protections.

### B. Independent Protection at Each Layer

In general, the protection scheme of layer $i$ is independent of that of layer $i+1$. With independent protection schemes at each layer, for a working path at layer $i$, the corresponding backup path is set up at the layer $i$. A working and its backup path of layer $i+1$ may use disjoint working paths at the lower layer $i$. As a result, a working path at layer $i+1$ is protected twice at layers $i+1$ and $i$, which results in redundant protection. Fig.2 shows an example of redundant protection, where bandwidth $4c_{new}$ is reserved at the core network for a single connection of bandwidth $c_{new}$.

### C. Common Pool Method

The redundant protection problem has been studied on the ATM over optical networks [9], [12]. The common pool method is proposed by Demeester to solve the redundant protection problem in the ATM over optical networks [5]. As the authors have mentioned, this approach is general, and thus can be applied to any multi-layer networks. The main idea of this approach is to set up the backup paths of layer $i+1$ on the spare network of the lower layer $i$. Therefore, with this approach, there is no redundant protection. Fig.1 describes the common pool method applied to a hierarchical network. A working path at layer $i+1$ sets up a working path at layer $i$, and the backup path at layer $i+1$ uses the backup path at layer $i$.

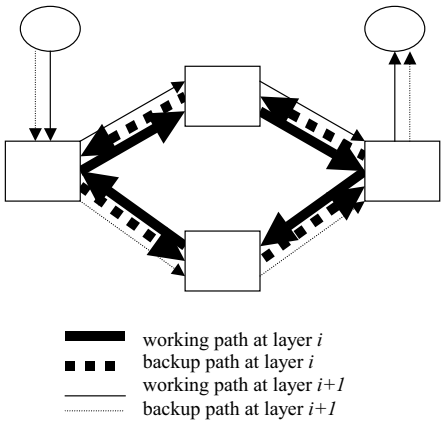


Figure 1. Common pool method

## III. Potential Problem of the Common Pool Method

### A. Potential Problem Description

The common pool method can protect any single link failure at any layer, while avoiding any redundant protection. However, for the concurrent two link failures, the common pool method cannot cope with. The most common example of two links failure problem is "two links failure at the same layer", which does not have any easy solution [4], [10]. This problem is well-known and has already been mentioned by Demeester [5].

In this work, we propose to consider a new type of two links failure problem, i.e. "two links failure at different layers". In general, the domain of layer $i+1$ is equal to or larger than that of the lower layer $i$. For example, the domain of MPLS network is larger than that of optical network. When the domain of layer $i+1$ and that of the lower layer $i$ do not completely overlap (i.e. non-overlapping layers), a link failure at the lower layer $i$ makes a part of the spare network of the layer $i$ busy. Since we now consider the common pool method, these busy elements of the spare network at the layer $i$ make the backup paths of the layer $i+1$ disabled until the failed link of layer $i$ is recovered. For example, for the MPLS over optical networks, a failure of an optical link can last

for several days [4]. Thus, once an optical link fails and the working optical paths are rerouted over the optical backup paths, there may be no backup paths for some label-switched-paths (LSPs) for several days. Moreover, when a shared protection scheme is used, the problem gets worse.

The cases that the common pool method fails are shown with examples in Figs. 2 and 3, where each optical link is assumed to support multiple LSPs, and only a single pair of working and protection LSPs are shown for easy illustration. A hierarchical network of MPLS over optical (WDM) network is shown in Fig. 2, and the failure of two links is shown in Fig. 3. In Fig. 3, the failure of optical link 1 makes the shared backup path in the optical domain busy, and the failure of optical link 3 cannot be protected any longer. This problem is well-known (i.e., the failure of atwo links at the same layer) [4]. We do not consider this problem in this work, but we consider another problem of "concurrent failures of two links at two different links", which may happen frequently in the MPLS over optical networks.

For example, in Fig. 3, the failure of optical link 1 makes the shared backup path in the optical domain busy. This protection mechanism in the optical layer does not leave any protection mechanism for the MPLS domain. This is because due to the common pool method, the spare MPLS network uses the spare network of the optical network. Thus, when the MPLS link 2 fails, there are no remaining backup paths for the related LSPs. The MPLS links are more apt to fail than the optical links in real scenarios.

The problem of "concurrent failures of two links at two different links" does not happen, given two independent protection schemes. Moreover, the frequency of failures and the recovery time of each layer are different. Considering these differences, in the following subsection, the probability of "concurrent failures of two links at two different links" are studied in depth.

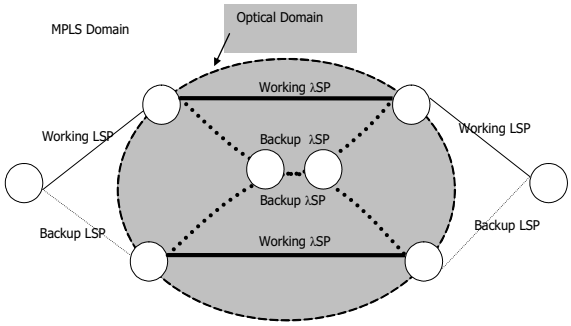


Figure 2. Hierarchical Network: MPLS over WDM

### B. Potential Problem Analysis

From Fig.4, based on simple Queueing analysis, the probability that both an MPLS link and an optical link

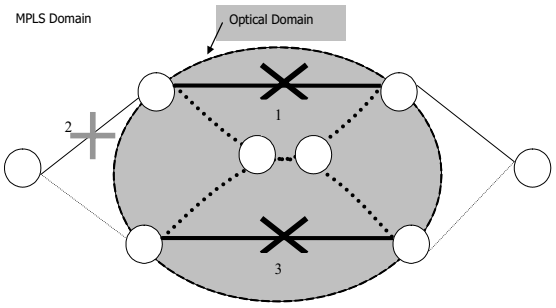


Figure 3. Potential Problem of the Common Pool Method

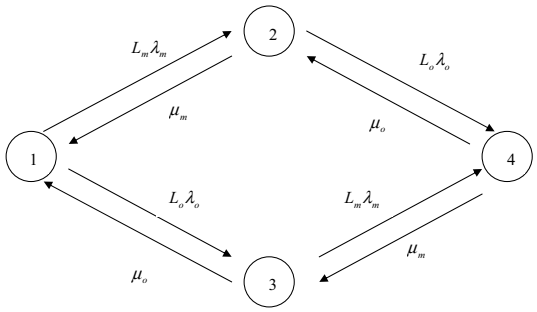


Figure 4. State Transition Diagram

fails concurrently is,

$$\begin{aligned} \text{P(fail)} &= \text{P(an MPLS Link Fail)}\frac{L_o\lambda_o}{L_o\lambda_o+\mu_m} + (1) \\ &\quad \text{P(an Optical Link Fail)}\frac{L_m\lambda_m}{L_m\lambda_m+\mu_o}, \end{aligned}$$

where state 1 indicates no link failure, state 2 an MPLS link failure, state 3 an optical link failure, state 4 indicates both MPLS and optical link failure, $L_o$ is total number of MPLS links, $L_m$ is total number of optical links, $\lambda_o$ is the rate of an optical link fails, $\lambda_m$ is the rate of an MPLS link fails, $\mu_o$ is the rate of an optical link recovers, and $\mu_m$ is the rate of an MPLS link recovers.

From Eq.(1), $\lambda_o$ is much smaller than the other factors, which results in P(fail) $\simeq$ P(an Optical Link Fail)$\frac{L_m\lambda_m}{L_m\lambda_m+\mu_o}$. $L_m$ is a large value and dominant over the other factors in the resulting equation. Thus, whenever an optical link fails, at least an MPLS connection may fail before the failed optical link recovers. The failed active MPLS connections cannot use the backup paths, thus the common pool method is not enough generally.

## IV. Proposed Protection Schemes

### A. Protection Scheme I

First, check if the domains of layer $i$ and $i+1$ completely overlap or not. When the domains of two layers exactly overlap, the problem of "concurrent failures of two links at two different links" does not exist

in these overlapping layers.

*Claim 1:* if the domains of layer $i$ and $i+1$ exactly overlap, the problem of "concurrent failures of two links at two different links" does not exist.

*Proof:* Since two layers share the same physical links in this case, a link failure of layer $i$ and $i+1$ does not happen separately. The problem of "concurrent failures of two links at two different links" corresponds to the problem of "the failure of two links at the same layer". Thus, in case the domains of two layers exactly overlap, the problem of "concurrent failures of two links at two different links" does not exist.

■

Based on *Claim 1*, this work proposes to use the common pool method for the overlapping two layers. In case that two sublayers do not completely overlap such as in Fig.5, two layers *i* and *i+1* are composed of an overlapping part and a non-overlapping part of layer *i+1*. Here, the non-overlapping topology is called the edge network and denoted with $T_e$, and the overlapping topology is called the core network and denoted with $T_c$. The full network topology of the layers $i$ and $i+1$ is denoted with $T_f$, where $T_f$ (= $T_e$ + $T_c$) [3].

*Claim 2:* if the domains of layer $i$ and $i+1$ do not exactly overlap (i.e., layer $i+1$ includes layer $i$), the problem of "concurrent failures of two links at two different links" may cause the common pool method to fail.

*Proof:* The proof is done with an example. Consider an MPLS over optical network, where MPLS and optical networks correspond to layer $i+1$ and $i$, respectively. In MPLS over optical networks that use the common pool method, when an optical link fails, the spare network of the optical network gets busy and fails to support backup LSPs of layer $i+1$. Thus, if an MPLS link fails before the failed optical link is recovered, some active LSPs cannot be rerouted since a part of the spare network of the optical network is now busy. Thus, the common pool method can fail in the problem of "concurrent failures of two links at two different links".

■

For the non-overlapping two layers, this work proposes to implant the independent protection mechanism in the core network and in the edge network separately. As a result, there are total three separated independent protection mechanisms such as in Fig.5. In the figure, there is an independent protection mechanism between $A$ and $B$, $B$ and $C$, and $C$ and $D$. Thus, when a link on the upper route between $A$ and $B$ fails, the traffic is rerouted to the lower route between $A$ and $B$. No other parts get involved in the restoration. For this proposed method to work, the working and backup paths of the edge network and those of the core network need to share a common node like nodes $B$ and $C$ in Fig.5.

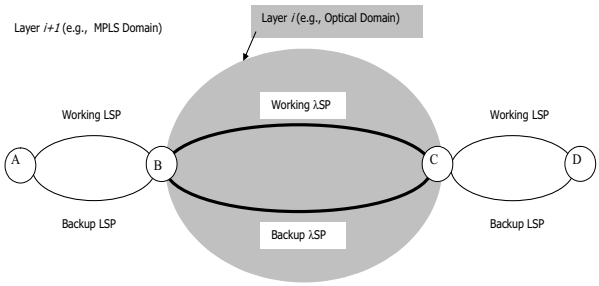


Figure 5. Network with Layers $i$ and $i+1$

With this proposed method, a link failure at the edge network (i.e. layer $i+1$) is recovered by the backup path of layer *i+1*, and a link failure at the core network (i.e. layer $i$) is done by the backup path of layer *i*. Thus, there is no redundant protection, and this mechanism does not fail at "concurrent failures of two links at two different links".

The proposed method, however, cannot be generally applied to GMPLS networks due to its topology constraints. Especially, it is not easy to guarantee two disjoint routes in edge network $T_e$. Thus, this proposed method is only appicable to the networks, where both edge ($T_e$) and core ($T_c$) network is 2-connected.

### *B. Protection Scheme II: Independent Protection structure for spare network (IPS)*

For a general solution, we propose to construct an additional independent protection structure at layer $i$, which can be used for the spare network of layer $i+1$. The Independent Protection structure at layer $i$, which is used only for the Spare network of layer $i+1$, is denoted with *IPS* structure. The *IPS* structure is shown with an example of MPLS over optical (WDM) network.

In the MPLS over optical networks, the *IPS* structure is constructed in the optical network, and independent of both working and spare optical paths. The *IPS* structure is not used by neither working nor spare optical paths. Thus, at an event of "concurrent failures of two links at two different links", the *IPS* structure suffers at most a single link failure. Here, the edge nodes of the optical network are called "optical access nodes", and the collection of the optical access nodes can be considered as an overlay network in the optical network, such as in Fig.6 [13].

*Claim 3:* if a link failure at LSP layer (i.e. layer $i+1$) causes a single working LSP to fail, the *IPS* structure only needs to guarantee the connectivity of a single backup LSP in WDM layer (i.e. layer $i$). This guarantee only requires the *IPS* structure to provide 2-connectivity between any two "optical access nodes" in WDM layer. If provided the 2-connectivity, the *IPS* structure can always provide the connectivity to

any backup LSP after an optical link failure in WDM layer.

*Claim 4:* if a link failure at LSP layer causes multiple working LSPs to fail, the *IPS* structure needs to guarantee the connectivity of these multiple backup LSPs in WDM layer. To do so, ($i$) the *IPS* structure is required to provide 2-connectivity between any two "optical access nodes" in WDM layer. Provided the 2-connectivity, the *IPS* structure can guarantee the connectivity to any single backup LSP after an optical link failure in WDM layer. Next, ($ii$) the *IPS* structure needs to guarantee to support multiple backup LSPs without causing any collisions.

There are many candidates for the *IPS* structure satisfying the conditions $i$ and $ii$ in *Claim 4*. For example, Hamiltonian protection cycle [7], two path protection scheme [2], two disjoint digraphs [10], optical network topology itself. The Hamiltonian network is the one that contains a Hamiltonian cycle in itself.

*1) Hamiltonian Protection Cycle (HPC):* The Hamiltonian protection cycle uses minimum network resources. To use Hamiltonian protection cycle, however, the network needs to be a Hamiltonian and 2-connected network. Every 2-connected network is recoverable from a single failure. Although, not every 2-connected network is Hamiltonian, however many networks are Hamiltonian [7]. In addition, networks can be made Hamiltonian by a design choice, and NSP and Pan-Europe backbone networks are Hamiltonian [7]. Therefore, the Hamiltonian protection cycle is preferred for the *IPS* structure. The other redundant protection structures also can be used similarly.

Thus in the Hamiltonian networks, a Hamiltonian protection cycle (HPC) can be built at layer $i$ as the *IPS* structure. This *IPS* structure needs to satisfy the 2-connectivity condition in *Claim 4*.

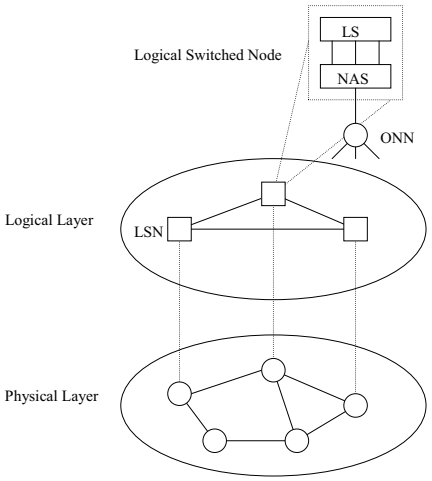


Figure 6. Logically Routed Network

The MPLS over WDM network can be modeled with the overlayed network like in Fig.6 [13], where *LSN* stands for logical switching node, *ONN* for optical network node, *ONN* for optical network node, *NAS* for network access system, and *LS* for logical system.

In Fig.6, the physical and logical layer corresponds to the optical and MPLS network, respectively. If the topology of the physical optical layer contains a Hamiltonian cycle, in the logical layer, the network access systems (NASs) can also form a Hamiltonian cycle among themselves, which is obvious. For convenience, instead of LSN, NAS is considered as the nodes of logical layer (MPLS network). The optical network can build a HPC that connects NASs with a pre-defined wavelength ($\lambda_{IPS}$). This HPC satisfies the 2-connectivity condition in *Claim 4*.

When multiple LSPs are to be rerouted at an MPLS link failure, there are collisions on the HPC of $\lambda_{IPS}$ because multiple backup LSP share the HPC. To cope with these collisions, this work proposes to use the functionality of NAS. Each backup LSP enters the optical layer through a NAS. Note that HPC is a ring structure, composed of multiple NASs (NAS 1, $\cdots$, NAS $n$). Consider NAS $i$ on HPC, which is busy due to the by-passing traffic (i.e. backup LSP traffic) from a neighbor NAS $i-1$. If a new backup LSP is set up through NAS $i$, NAS $i$ can combine these two traffic onto one.

That is, NAS $i$ first converts the by-passing optical traffic into the logical connection(LC) traffic with reception processor (RP) [13]. With transmission processor (TP), NAS $i$ can multiplex the by-passing LCs and the new arriving LCs. The multiplexed LCs can be converted into the optical traffic ($\lambda_{IPS}$).

Fig.7 shows the layered view of optical network connections and the detailed view of NAS, where *OT* stands for optical transmission, *OR* for optical reception, WMUX for wavelength multiplex, and WDMUX for wavelength demultiplex. For this functionality, each optical node only needs to handle as much traffic as that of the failed MPLS link, which is trivial to optical nodes.

By building up an independent HPC at the lower layer $i$, the proposed problem of "concurrent failures of two links at two different links" can be solved.

*2) Two Disjoint Spanning Trees (DST):* The two path protection scheme and two disjoint digraphs can be applied to more general networks. From Menger's theorem, for any vertex (edge)-redundant graph, there exists a pair of vertex (edge)-disjoint paths between any two vertices [10]. Thus two disjoint spanning trees can be found for every node [10]. However the cost of building this DST *IPS* is quite expensive because two spanning trees are to be set up for each node. Thus this *IPS* scheme is not practical at all.

*3) Optical Topology IPS:* The optical network topology itself can be used for *IPS* structure. That is, the so-called "optical topology *IPS*" can be built in the MPLS over optical network by reserving a pre-defined $\lambda$ ($\lambda_{IPS}$) at each optical link. Thus, if the optical network is 2-

TABLE I.
PWR COMPARISON OF THE FEASIBLE REDUNDANT MECHANISMS

| Topology $T_c$ [PWR] | Common Pool | Method I | Method II(HPC) | Method II(Optical Topology) |
|---|---|---|---|---|
| ring | 1 (faulty) | · | $\frac{AE-N}{AE+N}$ | $\frac{A-1}{A+1}$ |
| 2-connected Hamiltonian | 1 (faulty) | · | $\frac{AE-N}{AE+N}$ | $\frac{A-1}{A+1}$ |
| 2-connected non-Hamiltonian | 1 (faulty) | · | N/A | $\frac{A-1}{A+1}$ |
| 2-connected $T_c$ and $T_e$ | 1 (faulty) | 1 | · | $\frac{A-1}{A+1}$ |

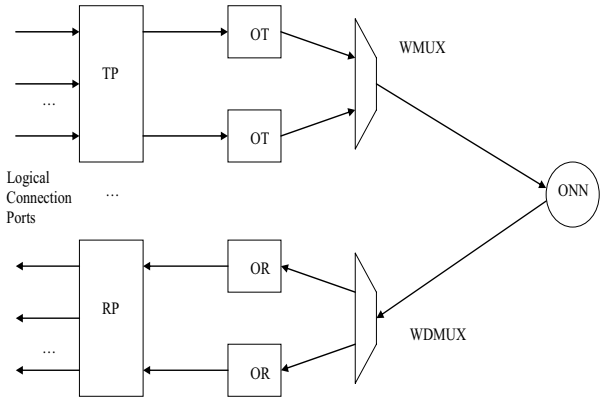


Figure 7. Detailed View of NAS

connected, the 2-connectivity is also guaranteed between any two optical access nodes due to the condition $i$ in *Claim 4*.

In case multiple working LSPs are to be rerouted, the multiple backup LSPs need to be set up without causing any collision among these backup LSPs. The functionality of NAS provides a solution on these collisions (refer Section IV-B.1). Thus, similar to HPC, multiple backup LSPs also can be controlled with an optical topology *IPS* due to the condition $ii$ in *Claim 4*.

By building up this "optical topology IPS" structure at the lower layer $i$, the proposed problem of "concurrent failures of two links at two different links" can be solved.

### C. Redundant Protection Comparison

To solve the "concurrent failures of two links at two different links", the proposed methods require an additional protection resourece (i.e. *IPS*).

We now evaluate the additional cost of the proposed method due to *IPS*. For the evaluation, we use the following metric: the protection to working capacity ratio (PWR) [8]. PWR is defined as the ratio of spare network resources (switch, port counts and link capacity) versus working network resources. For instance, with SONET self-healing ring, the working path is exactly duplicated into the backup path. The PWR of the SONET self-healing ring is thus 1. Due to the linearity of the cost function in the number of links, PWR=$\frac{N_p}{N_w}$, where $N_p$ and $N_w$ are the number of spare links and working links in the network.

Consider an MPLS over WDM network, in which the number of WDM nodes is $N$, that of WDM links is $E$, and each optical fiber carries $A$ [$\lambda$], where the unit [$\lambda$] means the number of wavelengths.

For the common pool method, when a one-to-one protection scheme is used (like the case of SONET self-healing ring), the working network is $\frac{AE}{2}$ [$\lambda$] and the spare network is also $\frac{AE}{2}$ [$\lambda$]. Thus, PWR = 1.

For the proposed method II with HPC, a $\lambda_{IPS}$ HPC is built at WDM layer as *IPS*. The HPC consists of $N$ hops, thus $N$ [$\lambda$] is reserved for *IPS*. Assume a one-to-one protection scheme is used in the WDM network. After setting up a HPC structure, among the remaining $AE-N$ [$\lambda$], $\frac{AE-N}{2}$ [$\lambda$] can be used for working and backup paths, respectively. As a result, the resulting working and spare network is $\frac{AE-N}{2}$ [$\lambda$] and $\frac{AE+N}{2}$ [$\lambda$], respectively. Thus, PWR = $\frac{AE-N}{AE+N} \simeq 1$, for $AE \gg N$.

For the proposed method II with the "optical topology *IPS*", a $\lambda_{IPS}$ is reserved at each optical link. Thus, total $E$ [$\lambda$] is reserved at the WDM layer for *IPS*.

Assume a one-to-one protection scheme is used at the WDM layer. After setting up *IPS*, among the remaining $(A-1)E$ [$\lambda$], $\frac{(A-1)E}{2}$ [$\lambda$] can be used for the working and spare path, respectively. As a result, the working network is $\frac{(A-1)E}{2}$ [$\lambda$] and the total spare network is $\frac{(A+1)E}{2}$ [$\lambda$]. Thus, PWR = $\frac{A-1}{A+1} \simeq 1$, for $A \gg 1$.

As a result, in terms of PWR, the addition cost of the proposed methods is trivial. The comparison results are summarized in Table I, where '·' symbol means that the corresponding method is feasible depending on the network topology, and '$N/A$' symbol means the corresponding method is not feasible.

## V. CONCLUSION

The redundant protection problem in multi-layer networks has been an interesting topic. Especially, this topic has been studied from the ATM over optical networks, and is newly focused on the IP over optical networks. Although the common pool method provides a simple solution for this problem, it can fail some cases. This work studies when the common pool method fails and shows that the common pool method cannot be directly applied to the GMPLS networks. This work also proposes a more general and simple solution to cope with these failures.

The proposed solution is (i) to separate the protection mechanism of each layer and run these mechanisms independently, and (ii) to build another independent protection mechanism at the lower layer $i$ for the redundant network of the layer *i+1*. The cost of building additional protection structure is minimal.

## REFERENCES


[1] D. O. Awduche, *"MPLS and Traffic Engineering in IP Networks,* IEEE Communications Networks, pp. 42-47, Dec. 1999.

[2] R. Bartos and M. Raman, *"A Heuristic Approach to Service Restoration in MPLS Networks,"* In Proc. of *IEEE ICC*, June 2001.

[3] T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, *"Introduction to Algorithms (Second Edition)," MIT Press and McGraw-Hill*.

[4] H. Choi, S. Subramaniam, and H. Choi, *"On Double-Link Failure Recovery in WDM Optical Networks,"* In Proc. of *IEEE Infocom*, June 2002.

[5] P. Demeester, M. Gryseels, A. Autenrieth, et al., *"Resilience in multilayer networks," IEEE Communications Magazine*, Aug. 1999.

[6] S. Jeon, *"Redundant Protection Problem in the Hierarchical GMPLS Networks,"* In Proc. of *IEEE LCN*, Nov. 2005.

[7] H. Huang and J.A. Copeland, *"Hamiltonian Cycle Protection: A Novel Approach to Mesh WDM Optical Network Protection,"* In Proc. of *IEEE HPSR*, 2001.

[8] H. Huang and J.A. Copeland, *"A Series of Hamiltonian cycle based solutions to provide simple and scalable mesh optical network resilience,"* newblock *IEEE Communications Magazine*, Nov. 2002.

[9] K. R. Krishnan, R. D. Doverspike, and C. D. Pack, *"Improved Survivability with multi-layer dynamic routing," IEEE Communications Magazine*, pp. 62-68, July 1995.

[10] M. Medard, S. G. Finn, and R. A. Barry, *"WDM loop-back recovery in mesh networks,"* In Proc. of *IEEE Infocom*, Mar. 1999.

[11] G. Mohan and C. Murthy, *"Lightpath Restoration in WDM Optical Networks," IEEE Network*, pp. 24-32, Nov./Dec. 2000.

[12] L. Nederlof et al, *"End-to-end Survivable Broadband Networks," IEEE Communications Magazine*, pp. 63-70, July 1995.

[13] T. Stern, *"Multiwavelength Optical Networks: A Layered Approach," Addison-Wesley*, Chapter 2, pp. 21-79, 1999.

[14] G. Swallow, *"MPLS Advantages for Traffic Engineering," IEEE Communications Magazine*, pp. 54-57, Dec. 1999.


**Sung-eok Jeon** received his B.S. degree in Electronics Engineering from Yonsei University, Seoul, Korea in 1996 and M.S. degree in Electric Engineering from KAIST, Taejeon, Korea in 1999. He is a Ph.D student in Electric and Computer Engineering at Georgia Tech. He did the mandatory military service in Korean army. His research interests include resource management, optimization, and wireless network modeling and distributed management.