Differentiated Multi-layer Survivability in IP/WDM Networks

H. Zhang, A. Durresi
Comp. & Inf. Science Dept., The Ohio State University
2015 Neil Ave., Columbus, OH 43210, USA
{zhangho, durresi}@cis.ohio-state.edu

Abstract

As the Internet and network technologies evolve, the IP over WDM solution has been envisioned as the most promising solution for the next generation Internet architecture. So survivability in IP/WDM networks becomes critical for the success of the next generation Internet architecture. Considerable research efforts have been dedicated to studying the survivability in IP/GMPLS and WDM network respectively, but still remains the need for a better understanding of the inter-working, coordination and functionality partitioning in survivability between IP and WDM. In this paper, we explore the necessity, methods and advantages to coordinate multi-layer survivability in IP/WDM network. We especially focus on the study of the escalation method, multi-layer network spare capacity design and function partitioning. We study the use of differentiated survivability policies combined with a multi-layer survivability scheme for IP/WDM networks.

Keywords

Differentiated multi-layer IP/WDM protection, Optical network protection, IP over WDM networks.

1. Introduction

As the Internet and transport network technologies such as WDM develop, the integration of IP and WDM by GMPLS [39] (a further generalization of MPLS [3] and MPλS [4]) offers the most promising solution to the increasing demand for network bandwidth, intelligence as well as manageability [1, 2]. In particular, GMPLS offers a powerful instrument for traffic engineering, constraint-based routing and many other advanced services such as VPN, required by future Internet applications.

With the upcoming of e-business, wide-area video-conferencing and many other Internet applications, it is expected that many business-critical transactions will take place over the Internet, which entails high availability, reliability and QoS guarantees from the network. So survivability of the IP/WDM networks is essential to the foundation and success of the next generation Internet.

In designing survivability options, there are many factors involved [16, 17]. The most important ones are: resource utilization, request blocking ratio,

0-7803-7382-0/02/$17.00 ©2002 IEEE

restoration/switching time, recovery ratio, recovery granularity, control complexity, tolerance of single or multiple faults and scalability. The ideal goal is to achieve maximum survivability with minimum recovery time, while maintaining maximum resource utilization. It is difficult to achieve all these goals at the same time and trade-offs between different solutions are needed. For example, dedicated protection schemes usually offer faster recovery than restoration schemes, but they are less resource-efficient on the other hand.

Considerable research efforts have been dedicated to the study of survivability mechanisms in WDM and IP/GMPLS network respectively [5-15]. But still remains the need for research focused on the inter-working, coordination and functionality partitioning of survivability mechanisms in IP/GMPLS and WDM. In order to provide a comprehensive and globally efficient survivable network service, an optimal integration between the survivability mechanisms at these two different layers is required. The survivability mechanisms in WDM layer are faster, coarser-grained (per wavelength or fiber) and more scalable than those in IP/GMPLS layer, but they cannot handle faults occurring at IP/GMPLS layer, such as router fault and service degradation in IP layer. On the other hand, the survivability mechanisms at IP/GMPLS layer besides handling errors at this layer they offer finer-grained service to different traffics, but they are usually slower and less scalable than their counterparts in WDM layer. For example a single WDM link failure might result in failure of thousands of IP layer traffic. Also knowledge of WDM layer topology is needed to guarantee WDM layer diversity for backup path in IP layer [18]. Therefore, it is natural to integrate the survivability mechanisms in both IP/GMPLS and WDM layers.

As the Internet is becoming the global communication infrastructure, there are a wide variety of applications with different requirements for network reliability running over Internet. It would be desirable to provide 100% resilience guarantee to all the traffic over Internet, but this is both unrealistic and unnecessary. For example some applications, such as email, do not need the same high reliability as real-time medical or banking information. Also it is not cost-efficient to provide equal resilience to all different type of traffics running over the Internet. Thus, it would be more realistic to provide different level of network survivability to different traffic types in accordance with the respective Service Level Agreement (SLA) and try to maximize the network utilization.

A better trade-off between survivability and network utilization can be reached by adapting the survivability mechanisms to the changing state of network resource, such as bandwidth. For example, when network resources are scarce, the survivability of lower priority traffic might be relaxed to accommodate more higher priority traffic. This is justifiable since network faults, such as fiber cut, in general are not very frequent event.

The rest of this paper is organized as follows. In section 2 we analyze the network architecture, IP/WDM network model and WDM transport network topology adopted here. In Section 3, we analyze the properties of different survivability schemes in both IP/GMPLS and WDM layers. Then in Section 4, we analyze in detail the differentiated resilience services required and the association of different survivability mechanisms with different traffic under different network state. We discuss the multi-layer survivability issues in Section 5. The conclusion and future work plan is drawn in Section 6.

2. IP/WDM Network Architecture

The integration of IP and WDM is facilitated by the development of GMPLS[39] as a generalization of MPLS [3] and its lambda variant MPλS [4]. By using lambda as the label for Label Switched Path (LSP), GMPLS offers an effective control plane alternative to optical network and provides the opportunity of seamless integration of IP and WDM. The lightpath created by GMPLS in optical domain works as a LSP tunnel for end-to-end LSP in IP domain [4].

There are basically three models for integrating IP/WDM networks: overlay model, peer model and integrated model [1, 2, 18, 19]. The overlay model is likely to be adopted in the near-term rapid deployment IP/WDM networks. Due to their overall simplified management and control structures, the peer and integrated models are likely to be adopted in the long run for highly dynamic IP/WDM networks, when supporting vendor hardware and software will be available [18]. In this paper, we only consider the overlay model. The schemes for multi-layer survivability in peer and integrated models are for further study.

The topology of WDM networks is another important architectural issue that needs careful attention when designing survivability mechanisms. There are mainly three different WDM topologies: point-to-point, optical ring and optical mesh [18, 20]. The mesh configuration is more flexible than the other options. It is shown in [20] that the cost reduction in 10 Gb/s optics would make the optical mesh architecture even more attractive. So, the next generation Internet backbone would be a flexible, reconfigurable and reliable mesh optical network with OXCs connected to one another. Consequently we only consider optical mesh network in this paper.

3. Survivability Mechanisms in IP/WDM Mesh Networks

Before exploring the differentiated and multi-layer survivability issues in IP/WDM network, we first summarize the different protection/restoration schemes in IP/GMPLS and WDM layers respectively

3.1 Survivability Schemes in WDM Mesh Networks

Extensive research work has been dedicated to survivability options for WDM mesh networks [5-10, 21-23]. Here we first present an overview of those survivability options, and then analyze their respective properties with respect to some evaluation criteria, such as protection switching/restoration time and capacity utilization.

Generally speaking, there are two basic paradigms for WDM mesh network [5-7], illustrated in figure 1: (a) path protection/restoration and (b) link protection/restoration.

Path protection/restoration

In path protection, the source and destination nodes of each connection statically reserve backup paths on an end-to-end basis during call setup. In path restoration, the source and destination nodes of each connection that traverses a failed link

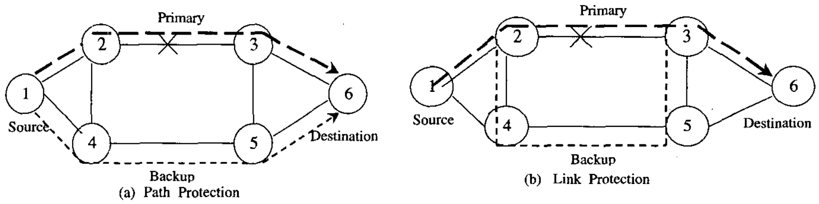

Figure 1: Protection schemes in WDM mesh network

dynamically discover a backup route on an end-to-end basis (such a backup path could be on a different wavelength channel) after the link failure.

- In *Dedicated-path protection* (1+1 or 1:1 protection), at the time of call setup for each primary path, a link-disjoint backup path and wavelength are reserved, and dedicated to that call. In 1:1 protection, the backup path could be used to carry other preemptible traffic, but when there is link failure in the corresponding primary path, the backup path will be used to carry traffic in the primary path again.
- In *Shared-path protection*, at the time of call setup for a primary path, a link-disjoint backup path and wavelength are also reserved. However, the backup wavelength reserved on the links of the backup path may be shared with other backup paths, which make this solution more cost effective than dedicated-path protection.
- In *Path restoration*, the source and destination nodes of each connection traversing the failed link discover a backup route and wavelength on an end-to-end basis; such a backup path could be on a different wavelength channel. The backup route is discovered either by some distributed algorithm using flooding [6] or by computation at the source node if it has QoS routing information about the WDM network.

Link protection/restoration

In link protection/restoration, all the connections that traverse the failed link are rerouted around that link. The link switch-over is transparent to the source and destination nodes. In link protection, during call setup, backup paths and wavelength are reserved around each link of the primary path. In link restoration, the end-nodes of the failed link dynamically discover a route around the link, for each wavelength that traverses the link. *Shared-link* protection and *link restoration* mechanisms work similarly as their path counterparts. *Dedicated-link protection* is not considered in this paper, because in general, it may not be possible to allocate a dedicated backup path around each link of the primary call, and on the same wavelength as the primary path [5].

Different survivability schemes mentioned above have different characteristics. Generally, link-level schemes provide faster recovery while path-level mechanisms provide better resource (such as bandwidth) utilization and higher restoration ratio. The protection schemes offer shorter recovery time while the restoration options offer better resource utilization. Usually, the restoration time is hundreds of milliseconds (200 ms or so), while the protection switching time is less than a hundred milliseconds (50ms or so). Also it is usually less complex to control

Table 1: Comparison of survivability schemes in WDM mesh network

WDM Survivability Mechanisms		*Resource Utilization*	*Protection Switching / Restoration Speed*	*Recovery Ratio (Efficiency)*	*Ease of Control*
Path Level	*Dedicated path Protection*	**	****	****	****
	Shared Path Protection	***	***	****	**
	Path Restoration	****	*	***	*
Link Level	*Shared Link Protection*	*	****	****	***
	Link Restoration	****	**	**	*

(Note: the more star in a block, the better the corresponding mechanism.)

protection that to control restoration. The detailed qualitative comparison result is shown in Table 1.

In protection schemes (path/link level, dedicated/shared), there are spare resources reserved for each protected part while those resources are not used under normal conditions. So restoration usually has better resource utilization than protection. Shared protection means multiple protected parts share the same spare resource, while dedicated protection means each protected part has dedicated spare resource. So shared protection schemes usually have better resource utilization than dedicated resource utilization.

As for recovery time, protection usually takes shorter time to recover from failure than restoration does. This is because the protection path has been found before failure, while in restoration it is needed to dynamically search for the alternate path. Link restoration tries to find the alternate path locally while path restoration tries to find the alternate path globally, so link restoration usually takes less time to find the alternate path. Path protection usually also takes longer time than link protection does.

During network failure, it is possible that not all the affected traffic could be restored. We refer recovery ratio (efficiency) as the ratio of the recovered traffic to the total of affected traffic. In protection scheme, the affected traffic is usually guaranteed to be recovered from failure because there is dedicated spare network resource for it, while in restoration scheme there is no such guarantee. So, protection schemes usually have higher restoration ratio than restoration schemes.

In view of control complexity, it is usually easier to control failure-recovery operation in protection schemes because the protection path has already been fixed beforehand while in restoration schemes, the alternate path is found on the fly, which means more coordination of network and more control.

3.2 Survivability Schemes in IP/GMPLS

In traditional IP networks, survivability is achieved by rerouting, which is flexible but slow due to the slow routing information convergence after failure. The introduction of MPLS/GMPLS into IP domain has offered chances of fast rerouting in IP networks, which does not necessarily require complete routing information convergence, especially in the case of single link or node failure. So, we only consider survivability schemes in GMPLS domain in this paper. Actually, the idea of traditional IP rerouting is also reflected in GMPLS path restoration.

A Label Switched Path (LSP) is a connection between an ingress Label Switching Router (LSR) and an egress LSR, consisting of a sequence of LSRs. Every packet going from the ingress LSR to the egress LSR has a label that uniquely identifies the path this packet should take. Upon arriving at each LSR in the LSP, the packet is switched according to the label it carries as well as the ingress port it arrives and it will be assigned a new label and sent to an appropriate outgoing channel along the LSP [3]. It behaves just like a lightpath in WDM network. So most survivability ideas or schemes in WDM network could be adapted to fit into GMPLS domain. But there are still some differences between GMPLS and WDM layer that need to be handled in survivability schemes. One major difference between a lightpath and a LSP is that a LSP could be reserved with zero resource, such as bandwidth, consumption, but whenever a lightpath is reserved, the corresponding wavelengths along the lightpath have to be reserved at the same time. Another difference is that a LSP is much finer-grained than a lightpath, which means more flexibility and complexity at the same time.

In [11-15] is presented extensive research about chances and possible options for survivability in GMPLS layer and they have proposed many survivability schemes for GMPLS. Similar to survivability schemes in WDM mesh network, there are basically two levels of resilience scheme in GMPLS, illustrated in figure 2: (a) Global protection/ restoration and (b) local protection/restoration.

The characteristics of different survivability schemes in IP/GMPLS are similar to those in WDM mesh networks. Generally, local schemes are simpler and provide faster recovery (protection-switching or restoration) while global mechanisms provide better resource (such as bandwidth) utilization and higher restoration ratio; and protection schemes offer shorter recovery time while restoration options offer better resource utilization. Usually, the protection switching time is under a hundred milliseconds (50ms or so), while the restoration time is much longer (hundreds of

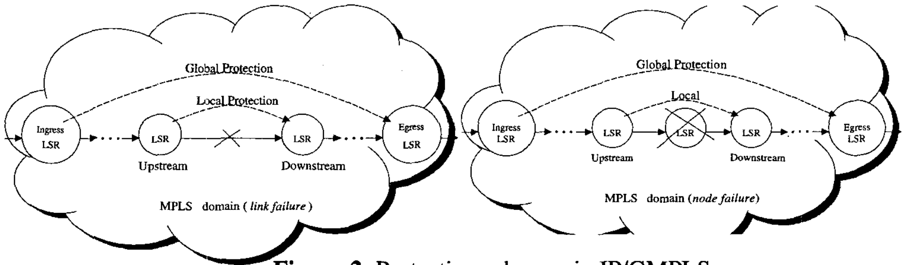

Figure 2: Protection schemes in IP/GMPLS

Table 2: Comparison of survivability schemes in IP/GMPLS

WDM Survivability Mechanisms		*Resource Utilization*	*Protection Switching / Restoration Speed*	*Recovery Ratio (Efficiency)*	*Ease of Control*
Global repair	*1+1 Protection*	**	****	****	****
	1:1 & 1:N Protection	***	***	****	**
	Restoration	****	*	***	*
Local repair	*Protection*	*	****	****	***
	Restoration	****	**	**	*

seconds), which are outstanding improvement upon the restoration time of tens of seconds in traditional IP rerouting [25]. The detailed qualitative comparison result is illustrated in Table 2.

4. Differentiated Survivability Service in IP/WDM Mesh Network

It would be desirable to provide 100% resilience guarantee to all the traffic over Internet, but this is both unrealistic and inefficient. Also it would be unreasonable to provide more than 100% capacity overbuild to guarantee 100% network availability for example to email traffic. On the other hand, business-critical online transactions might require very high network availability and reliability, because the cost of traffic losses in this case would be very high. So, in the new global and business oriented Internet an important requirement will be to provide differentiated survivability services to different types of traffic, with higher priority traffic enjoying higher network availability for the appropriate payment.

According to analysis in [16, 17, 26-29], the application traffic might be divided into four different categories requiring different levels of network survivability:

- *High-resilience-requirement traffic.* This type of traffic includes mission-critical VoIP or multimedia services, remote database transactions, critical control terminals and E-commerce applications.
- *Medium-resilience-requirement traffic.* Application traffic of this class includes Application Service Provisioning (ASP), standard VoIP and multimedia applications, etc.
- *Low-resilience-requirement traffic.* Traffic in this category includes e-mail, FTP or standard WWW, etc.

Besides providing differentiated survivability service by traffic type, the survivability policies might also be adapted according to different states of network resources, such as bandwidth, to make even better use of existing network resources. When network resource is abundant, higher availability guarantee might be provided to all the traffic; when network resources at a lower level, relatively high network availability might be provided to mission-critical traffic, while reducing the availability guarantee to the less critical traffic. This solution can lead to a better trade off between network utilization and protection of high priority traffic. Thus, the respective survivability schemes adopted in WDM and IP/GMPLS layers would depend both on the importance, priority of the traffic itself and on the network state.

Based on the idea of differentiated survivability service according to different traffic type and network state, together with the different characteristics of different survivability schemes in WDM and IP/GMPLS layers, we have developed a strategy about how to choose differentiated survivability services under different conditions (network state and traffic types) to maximize the network resource utilization. The differentiated-survivability-service policy in IP/GMPLS layer is illustrated in Table 3.

Under conditions of abundant spare network resources, it is reasonable as well as feasible to provide 1+1 or 1:1 global protection or local protection to traffic of high-resilience requirement to guarantee high network availability. For traffic with medium-resilience requirement, it would be provided 1:N global protection to guarantee relatively high network availability while do not waste network resource too much, enabling more traffic supported by the network. For traffic of low-resilience requirement, it is needed just to provide dynamic local restoration, because of its tolerance of network interruption and our purpose to use the network resources efficiently.

Under conditions of medium spare network resources, it is feasible to provide 1:N global protection for traffic with high-resilience requirement to conserve some network spare resource while still maintaining good enough network availability. For traffic of medium-resilience requirement, it is justifiable to provide local restoration with pre-computed backup path, thus providing fast recovery while minimizing spare network resource consumption. For traffic with low-resilience requirement, we only need to provide dynamic global restoration to maximize network resource usage while maintaining some survivability to the low-resilience-requirement traffic.

Table 3: Differentiated Survivability Services at IP/GMPLS layer

Requirement	*No (scarce) Network Resource*	*Medium Network Resource*	*Abundant Network Resource*
Low Resilience	*Traffic Dropped (no recovery)*	*Global Restoration (dynamic backup path discovery)*	*Local Restoration (dynamic backup path discovery)*
Medium Resilience	*Global Restoration (dynamic backup path discovery)*	*Local Restoration (pre-computed backup path)*	*1:N Global Protection*
High Resilience	*Local Restoration (pre-computed backup LSP)*	*1:N Global Protection*	*1+1 or 1:1 Global or Local Protection*

Table 4: Differentiated Survivability Services in WDM layer

Requirement	*No(scarce) Network Resource*	*Scarce Network Resource*	*Abundant Network Resource*
Low Resilience	*Traffic Dropped (no recovery)*	*Path Restoration (dynamic backup path discovery)*	*Link Restoration*
Medium Resilience	*Path Restoration (dynamic backup path discovery)*	*Link Restoration*	*1:N Shared Path Protection*
High Resilience	*Path Restoration (with pre-computed backup path)*	*1:N Shared Path Protection*	*1+1 or 1:1 Dedicated Path Protection or Shared Link Protection*

Under conditions of no or scarce spare network resources, it is reasonable to provide local restoration with pre-computed backup path for traffic with high-resilience requirement to maintain relatively fast recovery. For traffic of medium-resilience requirement, it might be provided dynamic global restoration to optimize usage of network resource while maintaining a certain degree of network survivability. The low-resilience requirement traffic might just be dropped to free some spare network resources for traffic requiring high network availability.
The differentiated-survivability-service policy in WDM layer is illustrated in Table 4. The analysis is similar to that for Table 3, so we leave it out here for brevity.

5. Multi-layer coordination for differentiated survivability services in IP/WDM mesh networks

When designing survivability schemes at both IP/GMPLS and WDM layers, it is required to coordinate carefully recovery actions at these two layers, otherwise unexpected results might come up due to the function duplication at both layers. For example, when a fiber cut happens in the network, there might be multiple fault notification information occurring at both layers, which results in parallel recovery actions at both layers. In this case, it might be unnecessary for IP/GMPLS layer to do any recovery action if the fault could be taken care of completely by WDM layer. But recovery actions at IP/GMPLS layer do happen if not coordinated properly, which means waste of network resources. Even worse the recovery actions at both layers might take place at the same time, when network resource is rather scarce. In this case there is resource (such as bandwidth) competition between IP/GMPLS and WDM and no recovery action at both layers might get the necessary resource to proceed. This can lead to failure to recover from the network fault, which might have been possible if there was no resource competition between the two layers.

In the next sections we will focus (a) recovery strategy in IP/WDM network: where to start recovery after failure, at IP/GMPLS layer or WDM layer? (b) what are the escalation mechanisms between WDM and IP/GMPLS layers? (c) multi-layer spare capacity design: how to design multi-layer spare capacity in the network?

5.1 Multi-layer recovery approach in IP/WDM network

There are two possible ways to recover from a network failure: recovery at IP/GMPLS layer or at WDM layer [30, 35, 36].

Recovery at IP/GMPLS layer has several advantages: (a) if a failure (either in IP/GMPLS layer or in WDM) in network could be recovered in any way, then it could be recovered in IP/GMPLS layer; (b) since survivability schemes in IP/GMPLS layer is finer-grained that those in WDM layer (a IP/GMPLS-layer single flow vs. a whole wavelength or optical fiber), it would be easier and more efficient to offer differentiated survivability in IP/GMPLS layer (as discussed in Section 4). On the other hand, recovery only at IP/GMPLS layer has some disadvantages: (a) recovery time at IP/GMPLS layer (above the order of hundreds of milliseconds) is usually higher than that in WDM layer (under the order of hundreds of milliseconds); (b) when a single fiber cut or other failure occurs at WDM layer, there might be thousands of IP/GMPLS traffic flows that are influenced by this failure. If it is adopted a recovery schemes at GMPLS layer to handle this kind of network failure, there would be thousands of recovery process at IP/GMPLS layer; however, if it is recovered this WDM-layer failure at WDM layer, only one recovery process involved. So recovery at IP/GMPLS layer is less scalable than that at WDM layer.

On the other hand, recovery at WDM layer has the strength that IP/GMPLS-layer survivability schemes lack. WDM-layer recovery is faster and more scalable than that at IP/GMPLS layer. But it has some disadvantages too, which coincide with the advantages of IP/GMPLS-layer survivability schemes. WDM-layer recovery cannot handle component failures at IP/GMPLS layer (such as IP router failure). It is coarser-grained than that at IP/GMPLS layer, thus less efficient at providing differentiated survivability service.

Based upon the analysis above, we could see that recovery at the lowest possible layer is better suited to IP/WDM networks. That is, (a) if a failure occurs at WDM layer, first it should be tried to recover it at WDM layer using corresponding survivability schemes at this layer; if this attempt fails, then it should be initiated recovery at IP/GMPLS layer; (b) if a failure happens at IP/GMPLS layer, it should be tried to recover it at IP/GMPLS layer only.

5.2 Interworking strategy between IP/GMPLS and WDM layers

Generally, two options were identified concerning the activation: starting the recovery schemes at different layers in parallel or starting them sequentially [30]. According to analysis in section 5.1, we will discuss the sequential escalation strategy in IP/WDM networks, because it has less control complexity. So, if a WDM-layer failure occurs, recovery actions at WDM layer and IP/GMPLS layer will be initiated sequentially, with WDM-layer actions initiated first. So the major problem is how and when to escalate the fault detected in WDM layer to IP/GMPLS layer.

References [35-38] suggested using a *hold-off timer* properly managed in IP/GMPLS layer to solve the escalation issue. The 'hold-off timer' is the interval between the detection of a failure at a LSR, and the generation of the first Fault Indication Signal (FIS) message, to allow time for lower layer protection to take effect. So, in order to avoid parallel recovery actions in IP/GMPLS and WDM layers, the hold-off timer should be long enough (in order of hundreds of milliseconds for WDM-layer restoration) to accommodate the time needed for WDM-layer recovery actions to finish, either succeed or fail. If it succeeds, no recovery action in IP/GMPLS layer is needed; if it fails, IP/GMPLS FIS is generated and recovery action in IP/GMPLS layer is initiated. More intelligently, the hold-off timer at IP/GMPLS layer might be adaptive to the traffic it carries, because different traffic with different resilience requirement is supported by different survivability schemes at WDM layer, which means different recovery times at WDM layer.

5.3 Spare capacity design in IP/GMPLS and WDM layers

Since transmission and switching resources are very expensive, optimization of spare resources is very important for both operators and users [30, 31]. Multi-layer survivability implies providing multiple spare capacity pools, each dedicated to a particular network layer. Since capacity of IP/GMPLS layer is carried by WDM layer, this results in a reservation of resources in all layers. Such redundant protection could be avoided by treating working and backup IP/GMPLS layer path (capacity) differently in WDM layers. In [30, 31] there are proposed the ideas of 'protection selectivity' and 'common pool' for ATM/SDH network, which could be introduced into IP/WDM networks little modifications.

'Protection selectivity' means that in the server layer, so WDM layer, the paths carrying client layer, IP/GMPLS layer, spare capacity can be left unprotected [30]. In this case, network resource requirements in WDM layer is reduced because not all IP/GMPLS capacity requires protection. But WDM layer still needs to dedicate some resources to carry the IP/GMPLS layer spare capacity. The utilization of the WDM layer resources can be further improved by sharing spare capacity across layers through the idea of 'common pool survivability' [30]. In common pool survivability, the spare capacity of the IP/GMPLS layer is treated as extra traffic in the WDM layer, thus is carried on unprotected preemptible paths. The spare capacity at the WDM layer is planned to protect the IP/GMPLS layer paths carrying the actual traffic. With common pool survivability, the WDM layer spare capacity is reused by a higher-layer recovery scheme. Little or not additional WDM layer resources are thus required to support the IP/GMPLS spare capacity, which is now carried in the reserve capacity provisioned for WDM layer survivability [30].

So, 'common pool survivability' enables better network resource utilization than both 'protection selectivity' and traditional schemes. It is appropriate for most traffic of medium or low network-resilience-requirements. But it might not provide adequate guarantee of network availability for traffic of high-resilience-requirement. For example, it is possible that some failures at both IP/GMPLS and WDM layers occur. Suppose the failure happens to 'primary LSP' at IP/GMPLS layer and to 'backup lightpath' at WDM layer. Both layers will adopt some form of recovery action. In the case of common pool survivability, the IP/GMPLS protection traffic is treated as extra preemptible traffic in WDM layer. So when IP/GMPLS layer initiates protection switching, there might be no WDM layer lightpath to support it, which leads to failing to recover the high-resilience-requirement traffic from network failure.

So, for traffic with medium or low network-resilience requirement, 'common pool survivability' should be used with the IP/GMPLS-layer protected traffic (capacity) treated as traffic with low-resilience requirement (see Section 4) in WDM layer. For traffic with high network-resilience requirement, 'protection selectivity' scheme should be used with IP/GMPLS-layer protected traffic treated as traffic with high or medium network-resilience-requirement in WDM layer (see Section 4).

6. Conclusion

Based upon WDM mesh network and overlay IP/WDM model, we first analyzed the properties of different survivability schemes in IP/GMPLS and WDM layers from the perspectives of network resource utilization, protection-switching time or restoration time, recovery ratio and control complexity.

Then we proposed and analyzed a differentiated network resilience service scheme for both IP/GMPLS and WDM layers by integrating these three factors: network resilience requirement, spare network resource state and different survivability schemes in IP/GMPLS and WDM layers.

Finally, we analyzed critical issues in multi-layer coordination for providing differentiated survivability services in IP/WDM networks, such as function partitioning, multi-layer recovery approach, inter-working strategy between IP/GMPLS and WDM layers and the spare capacity design in IP/WDM networks. The proposed solutions are based on differentiated survivability service in multi-layer IP/WDM architecture.

The ideas in this paper are mainly based on qualitative analysis. The next step we are going to take is to combine these differentiated multi-layer survivability ideas into underlying routing schemes and quantitatively analyze different schemes.

References

[1] J. Luciani, B. Rajagopalan, D. Awduche, B. Cain, and B. Jamoussi, "IP over optical networks: a framework", IETF draft, draft-many-ip-optical-framework-01.txt, July 2000

[2] N. Chandhok, A. Durresi, R. Jagannathan, R. Jain, S. Seetharaman, K. Vinodkrishnan, "IP over optical networks: a summary of issues", IETF draft, draft-osu-ipo-mpls-issues-01.txt, July 2000

[3] Eric C. Rosen, Arun Viswanathan, Ross Callon, "Multiprotocol label switching architecture", IETF draft, draf-ietf-mpls-arch-07.txt, July 2000

[4] Daniel O. Awduche, Yakov Rekhter, John Drake, Rob Coltun, "Multi-protocol lambda switching: combining MPLS traffic engineering control with optical crossconnects", draft-awduche-mpls-te-optical-02.txt, July 2000

[5] S. Ramamurthy, Biswanath Mukherjee, "Survivable WDM mesh networks, part I – protection", *Proc. IEEE Infocom* 99

[6] S. Ramamurthy, Biswanath Mukherjee, "Survivable WDM mesh networks, part II – restoration", *Proc. ICC* 99

[7] Ornan Gerstel, Rajiv Ramaswami, "Optical layer survivability – an implementation perspective", *IEEE Journal of Selected Areas in Communications*, Vol. 18, No. 10, October 2000, pp.1885-1889

[8] James Manchester, Paul Bonenfant, Curt Newton, "The evolution of transport network survivability", *IEEE Communications Magazine*, August 1999

[9] Ornan Gerstel, Rajiv Ramaswami, "Optical layer survivability: a service perspective", *IEEE Communications Magazine*, March 2000, pp. 104-113

[10] Chung-Sheng Li, Rajiv Ramaswami, "Automatic fault detection, isolation, and recovery in transparent all-optical networks", *Journal of Lightwave Technology*, Vol. 15, No. 10, October 1997, pp.1784-1793

[11] Thomas M. Chen, Tae H. Oh, "Reliable services in MPLS", *IEEE Communications Magazine*, December 1999, pp.58-62

[12] Ken Owens, Srinivas Makam, Vishal Sharma, Ben Mack-Crane, "A path protection /restoration mechanism for MPLS networks", IETF draft, draft-chang-mpls-path-protection-02.txt, July 2000

[13] Vishal Sharma, Ben-Mack Crane, Srinivas Makam, et al., "Framework for MPLS-based recovery", IETF draft, draft-ietf-mpls-recovery-frmwrk-01.txt, November 2000

[14] Li Mo, "General considerations for bandwidth reservation in protection", IETF draft, draft-mo-mpls-protection-00.txt, work in progress, July 2000

[15] Dimitry Haskin, Ram Krishnan, "A method for setting an alternative label switched paths to handle fast reroute", IETF draft, draft-haskin-mpls-fast-reroute-05.txt, November 2000

[16] Leo Nederlof, Kris Struyve, Chris O' Shea, "End-to-end survivable broadband networks", *IEEE Communications Magazine*, September 1995, pp.63-70

[17] Andreas Kirstaedter, Achim Autenrieth, "An extended qos architecture supporting differentiated resilience requirements of IP services", IETF draft, draft-kirstaedter-extqosarch-00.txt, July 2000

[18] John Y. Wei, Chang-Dong Liu, Sung-Yong Park, et al., "Network control and management for the next generation Internet", *IEICE Trans. on Communications*, Vol. E83-B, No.10, October 2000, pp. 2191-2209

[19] Ayan Banerjee, John Drake, Jonathan P. Lang, and Brad Turner, Kireeti Kompella and Yakov Rekhter, "Generalized multiprotocol label switching: an overview of routing and management enhancements", *IEEE Communication Magazine*, Jan. 2001, pp. 144-150

[20] S. Baroni, J. O. Eaves, M. Kumar, M. A. Qureshi, A. Rodriguez-Moral, and D. Sugerman, "Analysis and design of backbone architecture alternatives for IP optical networking", *IEEE Journal on Selected Areas in Communications*, Vol.18, No.10, October 2000, pp. 1980-1994

[21] Emmanuel Limal, Kristian E. Studbkjar, "An algorithm for link restoration of wavelength routing optical networks", *Proc. ICC* 99, pp. 2055-2061

[22] Georgios Ellinas, Aklilu Gebreyesus Hailemariam, Thomas E. Stern, "Protection cycles in mesh WDM networks", *IEEE Journal on Selected Areas in Communications*, Vol.18, No.10, October 2000, pp. 1924-1937

[23] Carmen Mas, Patrick Thiran, "An efficient algorithm for locating soft and hard failures in WDM networks", *IEEE Journal on Selected Areas in Communications*, Vol.18, No.10, October 2000, pp. 1900-1911

[24] Tsong-Ho Wu, "Emerging technologies for fiber network survivability", *IEEE Communications Magazine*, Feb. 1995, pp. 58-74

[25] Christopher Metz, "IP protection and restoration", *IEEE Internet Computing*, April 2000, pp. 97 – 102

[26] Hirokazu Ishimatsu, Yoshihiro Hayata, Susumu Yoneda, "Carrier needs regarding survivability and maintenance for switched optical networks", IETF draft, draf-hayata-ipo-carrier-needs-00.txt, November, 2000

[27] Fumito Kubota, Takashi Egawa, Hiroyuki Saito, et al., "QOS restoration that maintains minimum QOS requirements – a new approach for failure restoration", *IEICE Trans. Communications*, Vol. E83-B, No.12, December 2000, pp. 2626 - 2633

[28] Nada Golmie, Thomas D. Ndousse, David H. Su, "A differentiated optical services model for WDM networks", *IEEE Communications Magazine*, February 2000, pp. 68 – 73

[29] Eiji Oki, Naoaki Yamanaka, Francis Pitcho, "Multiple-availability-level ATM network architecture", *IEEE Communications Magazine*, September 1995

[30] Piet Demeester, Michael Gryseels, Achim Autenrieth, et al., "Resilience in multilayer networks", *IEEE Communications Magazine*, August 1999

[31] Johan Meijen, Eve Varma, Ren Wu, "Multi-layer survivability", white paper of Lucent Technologies, http://www.lucent-optical.com/ resources/, 1999

[32] K. R. Krishnan, Robert D. Doverspike, Charles D. Pack, "Improved survivability with multi-layer dynamic routing", *IEEE Communications Magazine*, July 1995, pp. 62 – 68

[33] Ken-ichi Sato, Satoru Okamoto, "Photonic transport technologies to create robust backbone networks", *IEEE Communications Magazine*, August 1999

[34] Shin'ichi Arakawa, Masayuki Murata, Hideo Miyahara, "Functional partitioning for multi-layer survivability in IP over WDM networks", *IEICE Trans. Communication*, vol. E83-B, No.10, October 2000

[35] Michael Cryseels, Satoru Ohta, Roberto Clemente, D. Piet, "Optimal design for service resilience in ATM over SDH backbone networks", *ATM Workshop Proceedings*, 1998 IEEE, 1998, pp. 400 -409

[36] Shanzhi Chen, Youxun Lei, Luoming Meng, et al., "An integrated restoration application (IRA) in the ATM network", 0-7803-4198-8/97, 1997 IEEE

[37] Ken Owens, Srinivas Makam, Ben Mack-Crane, "A framework for MPLS-based recovery", IETF draft, draft-ietf-mpls-recovery-frmwrk-01.txt, November 2000

[38] Robert Doverspike, Jennifer Yates, "Challenges for MPLS in optical network restoration", *IEEE Communications Magazine*, February 2001, pp. 89 – 96

[39] Peter Ashwood-Smith, Daniel Awduche, Ayan Banerjee, Debashis Basak, Lou Berge, Greg Bernstein et al., "Generalized multi-protocol label switching (GMPLS) architecture", http://search.ietf.org/internet-drafts/draft-ietf-ccamp-gmpls-architecture-01.txt