2006

Evolution of Protection Technologies in Metro Core Optical Networks

S. Chen
University of Wollongong, uow_chens@uow.edu.au

Publication Details
This article was originally published as: Chen, S, Evolution of Protection Technologies in Metro Core Optical Networks, International Conference on Networking and Services, 2006 (ICNS '06), 16-18 July 2006, 89.
Evolution of Protection Technologies in Metro Core Optical Networks

Abstract
The market of metro optical networking has increased rapidly over the last few years. Traditional telecommunication infrastructure has an emphasis on long-haul optical transmission with ultra broadband capacity, relying mostly on large pure Dense Wavelength Division Multiplexing (DWDM) systems. Today, however, metro core optical networks take the major role in provisioning local access services and interconnecting service points of presences (POPs) with long-haul transmission. This represents a pivotal point in business operations of data communication services for service providers and large enterprises. In addition, the upper layer data services completely leans upon the substrate wavelength communication, and hence the survivability and reliability issues in the optical domain are now becoming crucial topics. This paper provides a detailed discussion around the development process of protection technologies in metro core optical transport infrastructure.

Disciplines
Physical Sciences and Mathematics

Publication Details
This article was originally published as: Chen, S, Evolution of Protection Technologies in Metro Core Optical Networks, International Conference on Networking and Services, 2006 (ICNS ’06), 16-18 July 2006, 89.

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/453
Evolution of Protection Technologies in Metro Core Optical Networks

Sheng Chen
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
sc960@uow.edu.au

Abstract
The market of metro optical networking has increased rapidly over the last few years. Traditional telecommunication infrastructure has an emphasis on long-haul optical transmission with ultra broadband capacity, relying mostly on large pure Dense Wavelength Division Multiplexing (DWDM) systems. Today, however, metro core optical networks take the major role in provisioning local access services and interconnecting service points of presences (POPs) with long-haul transmission. This represents a pivotal point in business operations of data communication services for service providers and large enterprises. In addition, the upper layer data services completely lean upon the substrate wavelength communication, and hence the survivability and reliability issues in the optical domain are now becoming crucial topics. This paper provides a detailed discussion around the development process of protection technologies in metro core optical transport infrastructure.

1. Introduction
This paper presents a research of the recent history and potential future of optical protection technologies in metro core areas. Current data communication services are moving towards the efficient and cost-effective IP-oriented multiservice architecture. The concept of “IP over WDM” [1] is recognized as an ideal solution for supporting IP-oriented Next Generation Network (IP NGN) architecture. Therefore, the development of metro optical protection technologies is also extending from the single Time Division Multiplexing (TDM) plane to the unitive “IP+WDM” domain. In addition, future research will center on the interoperability between steady optical protection and intelligent IP restoration technologies.

2. Ring protection technologies in modern SONET/SDH systems
Since the SONET/SDH architecture was first deployed in TDM-based infrastructure, the metro ring topology with “1+1” has been chosen as a simple redundant solution. For instance, a Unidirectional Path Switched Ring (UPSR) network transport two ways of optical signals through a pair of fibers. One channel is called the working ring while the other is referred as a protection ring. Each ring carries the same traffic (i.e. “1+1”) throughout the entire SONET network which doubles the transport reliability. The protection ring will automatically switch the traffic within 50 ms in case of a failure (see Figure 1). Moreover, a Subnetwork Connection Protection (SCNP) structure also delivers identical protection mechanism in SDH network. This kind of protection approach provides a very fast response to network faults but 50% of bandwidth is wasted [2], and the significant disadvantage in that when both rings are disconnected by serious problems such as fiber cuts, the network operations will be totally suspended.

Figure 1. “2-fiber” UPSR with “1+1” path protection

Thus, a more flexible “1:1” protection approach was then developed. This scheme also utilizes 2N (N in courier) fiber-ring topology, however, the bandwidth in
each fiber is respectively divided fifty-fifty for both working and protection purposes. For example, in a Bidirectional Line-Switched Ring (BLSR, defined in SONET) or a Multiplex Section Shared Protection Ring (MS-SPRing, defined in SDH) architecture, the optical signals are exchanged and terminated between each node, and the bandwidth from every single network span can be reused if necessary. Once a failure occurs, the data traffic from one fiber is rotated at the error place and switched into another fiber (see Figure 2). As a result, the normal network operations will not be affected even if both fibers are get ruptured, while the available bandwidth in each individual span is also increased due to the resource reuse mechanism from the “1:1” protection principle. Because of the high efficiency and strong survivability, a four-fiber BLSR structure is the most popular deployment solution in current SONET metro backbones.

Figure 2. “2-fiber” MS-SPRing with “1:1” line protection

3. Resilient packet ring (IEEE 802.17)

To satisfy the requirements of next generation optical transport infrastructure, the latest layer 2 transport interfacing technologies such as Packet over SONET/SDH (POS) and 10-Gigabit Ethernet (10-GE) were developed to achieve the “IP over Optical” data service architecture. Since traditional optical protection techniques are mostly based on legacy TDM circuit plane, there is a distinct lack of protection and restoration mechanisms for ensuring the reliability of data packet services. Hence, the IEEE 802.17 work group has then released a fiber-ring based transport architecture, the Resilient Packet Ring (RPR), which is established on an innovative layer 2 MAC structure, named Spatial Reuse Protocol (SRP). The significance of SRP is that it allows re-encapsulating Ethernet frames into RPR frames, also referred to as “MAC in MAC”, which first empowers service providers to directly deliver the simple and efficient Ethernet services from LAN to WAN area. Based on this feature, RPR is also recognized a key transport technology in the emerging access service Metro Ethernet (ME) architecture [3].

In addition, RPR provides a superior restoration performance by implementing an Intelligent Protection Switching (IPS) approach, which is similar to that in BLSR or MS-SPRing structure (see Figure 3). Previously, the basic protection principle in conventional SONET/SDH networks relied on the pre-reserved protection bandwidth, which reduces the actual transport efficiency. However, the RPR architecture has its natural gift in bandwidth control and allocation which overcomes this technical gap while still keeping the restoration time under 100ms [4].

The SRP algorithm utilizes a destination stripping data transport mechanism instead of the inefficient method of passing tokens used in traditional ring-based data communication structures such as Token Ring and FDDI. Thus, data traffic is only added and terminated at defined source and destination nodes, which enables multiple concurrent flows from different parts of the ring. In addition, there is no specific pre-reserved protection bandwidth any more. As a result, this particular characteristic enhances the effective network operational bandwidth up to 100% level [5].

4. Fast reroute (FRR) technology

Nevertheless, as RPR is only dedicated to single-ring protection, it has an inborn limitation for protecting traffic across complex topology such as multiple rings or mesh structures. Thus, a more flexible protection solution, the Fast Reroute (FRR) technology has been introduced from IP/MPLS (Multiprotocol Label Switching) domain into metro core optical transport systems. FRR is an emerging protection scheme based on the Traffic Engineering (TE) feature of the mature IP/MPLS architecture. The basic
principle of FRR is to establish one or more bandwidth protection TE-tunnels along pre-specified Label Switching Paths (LSPs) to enable temporary bypassing of traffic in case of a link or node failure [6]. As demonstrated in Figure 4, when an IP packet comes to the head-end router, it simply encapsulates the whole packet with a pre-specified label header, which leads the packet across the working tunnel under normal circumstance. However, once the second node senses a link failure, it will directly switch traffic to the protection tunnel without any route recalculation. Because the original IP payloads and the label of working tunnel are wrapped again with the protection tunnel label header, the data traffic will be shifted to protection tunnels (LSPs) rapidly. Due to the intelligent protection mechanism, the frontal failure situation will be transparent to the head-end node, with almost no effect to the protected traffic in the working tunnel. Simultaneously, the second node will also send a path error message to notify the head-end node and give it time to recalculate a new, optimal route.

Moreover, by utilizing TE techniques such as Resource Reservation Protocol (RSVP) or Constraint-based LDP (CR-LDP) signaling protocols, FRR is able to provide end-to-end bandwidth reservation functionalities for TE-tunnels, which guarantees a strict restoration delay level for those specified key services in the situation of network failures. A latest lab test\(^1\) utilizing practical commercial equipments, connected with GE fiber links is able to demonstrate the actual protection performance of MPLS-TE FRR model. As shown in Figure 5, PE1 and PE2 are simulated as two head-end provider edge routers connecting with two customer routers (CE1 and CE2), along with a FRR enabled TE-tunnel established for ensuring the key layer 3 VPN traffic between the two branch sites. Concurrently, there is also simulated normal VPN traffic and public traffic injected into the two PE routers, without any specified protection approach.

By simulating two common (link and node) network failures, the results (see Table 1) shows FRR downgrades the maximum restoration time to a few seconds, while most of existing IP routing recovery solutions usually take tens or hundreds seconds to achieve re-convergence. However, there are noticeable distinctions of restoration time level between protected and normal services. For those specialized protected key services, FRR further reduces the restoration time to only one or two milliseconds grade.

<table>
<thead>
<tr>
<th>Test Type</th>
<th>Restoration Time</th>
<th>Key VPN traffic</th>
<th>Normal VPN traffic</th>
<th>Public traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE FRR Link Protection</td>
<td>&lt;2 ms</td>
<td>&lt;80 ms</td>
<td>&lt;200 ms</td>
<td></td>
</tr>
<tr>
<td>MPLS-TE FRR Node Protection</td>
<td>&lt;1.5 ms</td>
<td>&lt;2 ms</td>
<td>&lt;3.5 s</td>
<td></td>
</tr>
</tbody>
</table>

5. Overall considerations of current metro core optical protection

Based on the above discussion, an overall comparison of existing protection methods in metro optical transport field is provided as shown in Figure 6. Around the optical layer, only SONET/SDH and RPR

---

\(^1\) Tests and simulations were implemented on NGN network fast recovery test bed of China Netcom, 2005
protections can ensure strict restoration time within telecommunication requirements. However, both of them are inherently designed on a ring-based architecture, which means a scalability limitation when facing a complex topology. Although the SRP algorithm brings an attractive bandwidth utilization while keeping the telecom level restoration time for data services, it is helpless to TDM operation failures. This is due to RPR being designed to carry pure data packet services. Similarly, as MPLS-TE FRR offers a more comprehensive protection solution, it currently only supports data services such as GE fiber links.

Therefore, the protection techniques can be divided into two correlative control planes in current and near future metro optical networking field. For protections in the optical control plane, a practical approach is to combine RPR and traditional SONET/SDH protection methods together, for ensuring both data services and TDM operations. For protection in the data control plane, MPLS-TE FRR deployment can provide more flexible redundant solutions with guaranteed recovery time, especially for those pivotal services.

6. Future development orientations of metro core optical protection

6.1. WDM protection

In recent years, WDM protection has emerged as a scheme for first layer protection of metro core optical networks. Unlike fiber restoration of TDM systems, WDM protection focuses on the self-healing of internal wavelength channel connections. However, since the mature SONET/SDH systems are globally adopted, the protection of metro WDM networks is currently developed based on a TDM-based fiber ring architecture. The restoration operations of WDM rings is very similar to that of common TDM rings, such as the Unidirectional Wavelength-Path Switched Ring (UWPSR) and the Bidirectional Wavelength-Path Switched Ring (BWPSR) [7], whereas the resources of switching are now expanded to both fibers and wavelengths. However, some shortages from TDM systems are inherited by WDM protection such as the resources (wavelengths) wasted for reserved protection use. Network failures such as signal errors or fiber cuts are also detected in electronic domain back to the TDM layer, resulting in high complexity and low efficiency for the wavelength layer protection. Hence, current WDM protection is pressed for a set of independent and systematic mechanisms in terms of fault detection and service restoration.

Relying on legacy TDM ring architecture is a primary limitation in the development of WDM protection. For many years practical metro deployment, optical ring architecture has been recognized as an ideal topology for achieving the balance between efficiency and reliability. However, there is little doubt that the mesh design will be an ultimate stable solution, and it has already been approved as an ideal choice for protecting WDM networks [8]. Fortunately, present DWDM technology enables the combination of both topologies, which is to build logical wavelength mesh connections above physical fiber ring infrastructure. The latest Supercontinuum light source and Arrayed Waveguide Grating (AWG) techniques empowers the carrying capacity up to 1000 channel wavelengths over 120km on field testing [9,10]. This actually means the available amount of wavelengths now is sufficient to support about forty branches under full mesh deployment, while most of existing commercial metro DWDM systems can only support six to nine branches (sixteen to forty channels). In addition, with the global exploding demand of IP NGN data services, it is reasonable to believe that the physical (fiber) mesh will be first deployed in metro core transport area in a visible future. Under this circumstance, WDM protection is an ideal substitute solution for maximizing the system resiliency and survivability at the optical layer.

6.2. GMPLS-TE end-to-end protection

At the data control plane, as discussed in section 6.1, MPLS-TE FRR is currently recognized as a flexible and reliable protection solution, especially for specified data services. Nevertheless, the establishment of TE tunnels requires strict uniform MPLS configuration environment, mostly within a local Interior Gateway Protocol (IGP) domain. Additionally, the FRR functionalities are only supported by high level IP/MPLS routing equipment, which means the protection LSPs can not drill through in intermediate
non-routing environments such as the TDM network connection. Therefore, the concept of FRR has been introduced into Generalized MPLS (GMPLS) architecture [11]. GMPLS is indeed an extension of MPLS from IP to optical world, and it first enables the control and management from IP routing domain to the TDM and WDM optical transport layer within a common environment. Nowadays a metro core telecommunication infrastructure in large ISPs or enterprises may involve various network elements, such as IP routers, routers with TDM (ATM/FR) interfaces, Optical Add/Drop Multiplexers (OADMs) and Optical Cross Connects (OXCs). Inspired by the bright feature of FRR in MPLS, GMPLS then aims to utilize extended TE signaling protocols such as Generalized RSVP and Generalized CR-LDP, to establish non-blocking end-to-end protection tunnels through from packet switching to TDM switching to Lambda/Fiber switching domains [12]. Based on this extended TE architecture, GMPLS is capable of unifying the protection and recovery approaches between data service network and optical transport infrastructure.

Figure 7 gives a deployment landscape of future metro optical transport backbone. For the core layer, WDM mesh architecture is adopted as the steadiest protection solution with highest system resilience. For the distribution layer, there are many independent protection methods are selected for particular services from each autonomous span, such as the SONET/SDH ring protection for TDM operations, RPR ring protection for data services, or the combination of WDM and RPR for ensuring ROADM-based MSTP (next generation SONET/SDH) service transportation. Under this circumstance, however, GMPLS focuses on the holistic stability of extended TE tunnels between every head-end (provider edge) node, regardless of any intermediate network (IP, TDM or WDM) failure within a uniform GMPLS-TE domain. By exchanging standard TE extension signaling, each network element in front of a failure will automatically bypass the protected traffic through local restoration link, path or tunnel. Concurrently, the network element is also able to notify the head-end nodes immediately and give them time to recalculate for new optimal LSPs. Moreover, there is no conflict for introducing FRR into GMPLS-TE domain, and FRR can also be referenced as a local restoration technique to enhance the interoperability between MPLS and GMPLS.
6.3. Summary

Figure 8 gives a summary of protection technologies in future metro core optical networks. Firstly, WDM protection will be gradually adopted at the first layer with the efficient mesh architecture. Concurrently, RPR will also replace the SONET/SDH protection based on existing metro ring architecture, as IP-oriented data services will soon take the place of legacy TDM operations. In addition, a lot of vendors are now working on embedding the RPR feature into their existing metro transport and core routing systems as a standard configuration, which decreases the potential deployment investment significantly.

Secondly, the principle of TE-tunnel protection of FRR will be expanded from MPLS-TE to the uniform GMPLS-TE domain. By implementing standard TE extension signaling between all network (IP, TDM and WDM) elements, future service providers will be able to deliver veritable end-to-end data services with high guaranteed reliability through an entire metro span. By comparing with Figure 6, it is not hard to find that the future trends in the research on metro core optical transport reliability will focus on the convergence of WDM protection efficiency and IP/MPLS recovery resiliency.

7. Conclusion

The performance of network protection technologies reflects the stability and reliability of the whole carrier system. Present metro optical backbones require extreme operational safety, as they are ensuring various upper layer network services in various geographic contexts. Thus, this paper provides a comprehensive study on existing metro optical protection technologies, including the evolution from traditional SONET/SDH system to the emerging RPR architecture. A simulation under the FRR protection model within a MPLS-TE test environment is also supplied to demonstrate the practical performance of this emergent protection scheme. By providing a correlative analysis on the latest optical protection technologies, this paper clarifies the potential orientations for future development of metro core optical transport protection, that is, to simplify the protection operations and optimize the protection structures between IP (MPLS) and optical (WDM) control plane.

References