**Novel Design of G.ODUSMP to Achieve Sub-50 ms Performance with Shared Mesh Protection in Carrier Networks**

Wayne Wauford(1), Soumya Roy(1), Onur Turkcu(1), Satyajeet Ahuja(1), Steve Hand(1), Abhinava Sadasivara(1), Biao Lu(1)

(1) Infinera, Sunnyvale, California, USA, email: wwauford@infinera.com

**Abstract** This paper describes the first practical implementation of shared mesh protection with <50 ms performance using the emerging standards G.808.3 & G.ODUSMP. It also presents the performance benefits of this implementation demonstrating 20-26% network cost savings vs. 1+1 protection and a maximum protection switch time substantially less than 50 ms.

**Introduction**

Since the emergence of DWDM networks, 1+1 λ/ODUk SNCP protection has been the only solution that provides reliable <50ms protection switching performance over a wide range of network topologies. The drawback to 1+1 protection is the need to dedicate 200% of the service bandwidth in the network.

In the early 2000’s, IP-like control plane implementations (primarily ASON or GMPLS-based) were deployed. These schemes dynamically reroute services after a working path failure using available network bandwidth to restore the service, if possible. These mechanisms are very efficient in terms of bandwidth utilization because all unused network bandwidth is treated as a pool of shared protection resources. The short-coming of these mechanisms is that protection switching performance is highly variable, typically greater than 50ms, and greatly impacted by the complexity of the network topology and the number of services.

The newly emerging ITU standards for shared mesh protection, G.808.3 and G.ODUSMP, when coupled with hardware-based acceleration of the control plane functions can provide the best of protection mechanisms described above: <50 ms switching time and shared protection resources.

Prior works [3], [4], describe shared mesh protection, but this is the first paper to describe a practical implementation of shared mesh protection with <50 ms protection performance. We present two sets of modeling results describing a) cost savings in a reference network vs. 1+1 protection and b) protection switching performance as a function of number of simultaneous failed services recovered and length of recovery path.

**Shared Mesh Protection**

The G.808.3 [1] and G.ODUSMP [2] draft standards define a protection mechanism called “shared mesh protection” that predefines and pre-signals one or more logical protection paths for a service in a mesh network. However, these logical protection paths are not pre-provisioned, so they don’t dedicate network resources to any specific service. Therefore, many services can have logical protection paths that share the same resource(s) in a pool of reserved shared protection bandwidth. The working paths should be disjoint such that only one of the protection paths will use the resource(s) for a specific failure scenario.

![Dedicated Protection vs. Shared Protection](image)

**Fig 1**: Dedicated protection vs. shared protection

The first step in an implementation of shared mesh protection is determination of the logical protection paths required in a network. An integrated network planning and service provisioning application determines the logical protection paths required per service to provide the defined SLA (service level agreement): a) protection against all single failures, b) protection for a subset of failures, c) protection against multiple failures. Additionally, the planning algorithms ensure that for each failure scenario, two or more logical protection paths do not use same shared resource. The process above also determines what additional shared resources need to be reserved.

After planning, each logical protection path is signaled, using GMPLS, to all the network...
elements participating in the logical path. Based on
this signaling, each node pre-configures, but
does not implement, the required cross-
connects to set-up the protection path (Fig 2).
This enables fast implementation of the
protection path when needed.

**Fig 2:** Establishing logical protection paths for
different failure scenarios before a failure occurs

**Hardware Acceleration of Path Activation**
The use of predefined and pre-signaled logical
protection paths architecturally eliminates
several steps that have made existing
GMPLS/ASON dynamic reroute implementations slow and variable in
performance: the route computation is already completed and the cross-connects in the node
are already calculated. However, to guarantee
<50ms protection performance for longer paths,
e.g., 10 hops and for 1000’s of services
impacted by a failure, both a) the activation
messages must be processed and forwarded, and b) the protection path cross-connects must
be implemented within 2 to 3 ms per node. To
achieve this performance, real-time control
processor(s) are dedicated to these real-time
tasks. Using this dedicated hardware removes
the performance constraints found in software-
based methods.

**Fig 3:** Bi-directional protection activation with
hardware acceleration

Another performance enhancement is the use of
bi-directional path activation. Upon failure
detection, nodes at both ends of the service
start the activation of the protection for faster
convergence.

At each node receiving the activation message,
the real-time control processor(s) forwards an
activation message to the next node in the logical
protection path, and implements the pre-
calculated cross-connects to establish the
protection path in 2-3 ms (as shown in Fig. 3)

**Simulation Results**
A representative national network for Germany
was used to evaluate economics and
performance of this new approach (Fig. 4).

**Fig 4:** German Network Topology Details

**Network and Traffic Details**
The end-to-end optical express paths are
designed based on the real fiber characteristics
and all optical performance limitations are
simulated.

**Table 1:** Annual Traffic Growth Rate

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Annual Growth</th>
<th>YR 1 Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional</td>
<td>35%</td>
<td>30%</td>
</tr>
<tr>
<td>Data Center</td>
<td>50%</td>
<td>63%</td>
</tr>
<tr>
<td>Overseas</td>
<td>25%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Regional, overseas and data center traffic
models are aggregated to represent traffic
patterns seen in today’s network.

Regional traffic between cities a, b follows a
gravity model and is represented as

\[
t_{a,b} = T \times \frac{P_a P_b}{\sum_{i,j \in C} P_i P_j / d_{i,j}}
\]

C: Set of cities, T: Year 1 Traffic,
P_a, P_b: Population of cities a, b.

Data center traffic between cities has been
estimated using market research data.

Overseas traffic entering the network through a
cable landing site C_i (e.g., i) is distributed to
eyery city proportionally only to its population
(e.g., i = T_i^{C_i} P_a/\sum_{j \in C} P_j). T_i^{C_i}
values are obtained from market research.

Based on the service mix obtained by the
market analysis, the total bandwidth demand
between a pair of nodes at the end of each
growth period is assigned to service interfaces
(1G, 2.5G, 10G, 40G, and 100G). Total interface
traffic in Year 1 is 8.3Tb/s.

**Simulation Setup**
We compare resources for three options:
a) Unprotected only: shortest path between
destinations, b) 1+1 protected: shortest path for
working, and second shortest path for
protection, c) Shared mesh protected (SMP):
resources like timeslots for protected paths are
shared among services while ensuring that
network is resilient to single-link failures. Over
all services affected by the single link failure, the
aggregate protection bandwidth requirement on each wavelength is calculated (denoted by $\text{Protection}_{BW_{w,l,f}}$; BW requirement on wavelength $w$ of link $l$ for failed link $f$). This calculation is repeated by simulating all link failures in the network. The maximum Protection Bandwidth requirement is then calculated:

$$\text{Max Protection}_{BW_{w,l,f}} = \max_{f} \text{Protection}_{BW_{w,l,f}}$$

### Simulation Results

Figure 5 shows the resources used by each scheme. Typically, the working path is the shortest path and the protection path is longer. Therefore, more than a doubling of resources is needed to add 1+1 protection. In contrast, SMP shares protection resources among multiple services and, in the German network, provides 20-26% savings compared to 1+1 protection.

![Fig 5: Savings with Shared Mesh Protection](image)

This shows that SMP provides significant savings in building a failure-resilient network compared to 1+1 protection. The resources needed for 1+1 protected and SMP scenarios both increase each year, but the SMP savings continues, although not linearly. This is because the unused bandwidth in the working path is used differently by the two schemes.

### Restoration Time Measurement

We have used CSIM, a discrete-event simulator [5], integrated with our network planning tool to simulate the message processing as it happens in hardware-accelerated control plane and measure the total restoration time after failures. CSIM time interval between a failure and SMP path set-up is measured for all demands impacted in a failure.

![Fig 6: Recovery Time vs. # of Impacted Demands](image)

Figure 6 plots the maximum, minimum and average restoration time of all demands affected following each failure. As evident, the restoration time is always significantly less than 50ms. Impact of queuing and processing delay is minimal because of hardware-based implementation even in the case when 450 demands are impacted and the number of hops is high. The fault detection time for these scenarios is always less than 2-3ms.

![Fig 7: Recovery time vs. distance and hops](image)

Fig. 7 shows the variation of restoration time with distance and hops. Restoration time increases with distance of the restoration path. Also, the graph shows that for the same hop and same distance, the restoration time varies markedly. This is because with different fault locations, bidirectional activation messages initiated from source and head nodes converge at different points on the restoration path. The best case is when activation messages converge at the middle of recovery path and the worst case is when it happens at the end. Also if the distance is the same, the impact of hop counts on the restoration time is minimal because of fast processing of activation messages.

### Conclusions

The shared mesh protection architecture coupled with hardware accelerated path activation, as shown in this paper, provide a more efficient and agile optical network that is adaptive to network events, while also providing deterministic, <50 ms protection performance. This enables carriers to move beyond the static transport networks deployed today without compromising service levels.

### References


