FastSMP™: Fast Shared Mesh Protection

Deterministic Network Resilience without the Expense

Synopsis Network resilience is a key requirement for 21st century service providers, as the ability of any system to recover from a failure is critical to meeting the customer expectation of 24 x 7 operations. The interdependence of business processes and the network, combined with an increasing number of natural disasters and man-made fiber cuts, has made the ability of the fiber infrastructure to quickly recover vital. Service providers are moving towards mesh-based transport networks to provide more backup path options. To help take advantage of this architectural shift and deliver more reliable networks for lower cost, Infinera has developed a new capability called FastSMP™, extending standards-based Shared Mesh Protection. This technology leverages an intelligent GMPLS control plane so a meshed transport network can recover from multiple local and network-wide failures while lowering costs by avoiding the need to dedicate backup bandwidth for every active circuit. Infinera uses a purpose-built hardware acceleration chip included in every single card of the DTN-X, guaranteeing a sub 50ms recovery end-to-end across the network, even in the face of multiple failures.
The Need for Network Resilience

Network bandwidth is growing at staggering rates, estimated at 40% growth year over year, driven by business applications like cloud, mobile, and video technologies. At the same time, the importance of network connectivity has never been greater, with virtually every business process now completely intertwined with network connectivity along with mission critical social, safety and local government services in most countries.

Both submarine and terrestrial networks are vulnerable to accidental, or in some cases, deliberate outages. Natural disasters seem to be increasing in frequency and intensity, often knocking out multiple fibers simultaneously. In 2008, a series of high profile outages in submarine cables connecting India and the Middle East with Europe were so frequent that there was widespread speculation that they were caused by terrorist activity. In 2009, four simultaneous fiber cuts in San Jose, California took out 911 services for an entire day. In 2011, a tsunami in Japan took out multiple submarine and terrestrial cables. In 2012, Hurricane Sandy took out multiple cables on the Northeastern seaboard of the United States.

In terrestrial cable systems, “failure by backhoe” is still the number one problem – especially in countries whose infrastructure is developing rapidly, and where planning records tend not to be up to date. In fact, in India, some service providers claim that they see as many as 100 fiber cuts per day nationwide. Many outages are caused by simple manual errors—such as an engineer unplugging the wrong fiber when they are making changes in the PoP. Even in highly developed nations, service providers can face interesting challenges. According to a Level3 blog post, 28% of their cable breaks in North America in 2010 were caused by squirrels chewing through the cables! A single outage of just 50 minutes in a year knocks network availability down to four nines, or 99.99%.

Protection versus Restoration

Whatever the reason for network outages, it falls to the service provider to fix the problems. In this effort there are generally two approaches:

• **Protection.** This must occur within 50ms of the failure. In order to achieve this rapid response, it is typical to use a pre-computed path for protection circuits. Protection capacity may be dedicated, or it may be switched. However, there are quite stringent limitations for traditional switched protection protocols in terms of topology and scalability. There may also be limitations on protecting against multiple failures.

• **Restoration.** In a restoration operation the fault is detected, a new path is computed, and connections are taken down from the working path and reestablished on the protection path. Restoration is common in packet networks, and while it may be comparatively slow (typically measured in seconds to minutes), it allows protection capacity to be shared, and will almost always find a way through as long as a backup path exists. Restoration is also possible at the digital transport layer, where the performance can improve from hundreds of milliseconds to a few seconds but still falls far short of the sub-50 millisecond failure recovery requirement.
Applying Resilience in the Network

50ms is the accepted and entrenched “gold standard” to meet in order for service providers to advertise such a service as “protected,” and charge an appropriate premium. For many years the most common way to achieve sub-50ms protection was by using SONET/SDH 1+1 protection. With “1+1” protection, the signal is sent over both the working path and the preconfigured protection path simultaneously so that 50ms can be achieved. However, this approach is expensive because it is necessary to reserve 100% of pre-configured protection capacity, and it is limited to protecting against only one failure in the working path.

As we have seen, networks are now facing multiple failures and single failure protection is no longer sufficient. Additionally, solving a multi-failure scenario is simply too costly in the face of rising traffic across fibers that can be carrying up to 8 Tbps of capacity. The pricing pressures faced by service provider business models demand a new approach to resilience.

The ideal resilience technology for modern transport networks should offer three fundamental capabilities:

1. Multi-failure recovery for better survivability;
2. Fast recovery within 50ms for deterministic performance; and
3. Intelligent sharing of backup resources for better economics.

If all three capabilities were available in a single technology, this would offer service providers the opportunity to create tiered protection plans, which could help to generate additional revenue for a minimum investment in protection capacity.

What are the current resilience techniques in common use, and how do they match up? They include the following:

- **SONET/SDH**: 1+1 and Sub-Network Connection Protection (SNCP) uses dedicated protection bandwidth to provide guaranteed sub-50ms protection for all payload types (SONET/SDH, Ethernet, SAN, video). This protection is used in the transport networks of many carriers today. As described above, this type of protection defined the 50ms value, but it does not offer protection against multiple failures, and the way that it is implemented normally means that protection capacity cannot be shared by other services.

- **Digital OTN/GMPLS**: Software Mesh Restoration is provided by newer intelligent optical cross-connect switches as an alternative to using dedicated bandwidth for protection. When a failure occurs, these devices use intelligent control planes to reroute the affected services using software-based tables that use unallocated bandwidth in the network. Since all unallocated bandwidth is available as a shared pool of restoration bandwidth, this mechanism is typically 20-35% more efficient in terms of network resources as compared to dedicated protection bandwidth. In addition, because GMPLS mesh restoration dynamically reroutes a failed service...
based on available bandwidth, this procedure can be repeated in the case of multiple failures in the network. However, the multi-stage, software-only approach can take seconds to recover and overall restoration time will increase with the complexity of the network topology, the number of links, and the number of restorable connections.

- **Packet IP/MPLS: Fast Re-Route (FRR)** is a router-based protection used in data-centric networks. Like GMPLS mesh restoration, MPLS FRR uses shared protection bandwidth for network efficiency and can recover from multiple failures. One of the goals for MPLS has always been to offer enhanced resilience compared to connectionless IP networks. MPLS FRR (sometimes referred to as MPLS Local Protection) allows a Label Switch Router the possibility to react within 50ms with a local detour once it detects a fault on the working path. MPLS FRR uses pre-computed Label Switched Paths and label values, so all that has to be done is that an LSR uses a new label and directs the traffic out of a different port. MPLS FRR allows an arbitrary topology to be used and is a shared protection technique. The drawbacks with MPLS FRR are that sub-50ms operation is not fully deterministic because it is only local and once the failure occurs, the entire network may need to re-converge, and that it makes use of additional expensive IP/MPLS router ports to achieve resilience.

The Case for Fast Shared Mesh Protection

Infinera’s Fast Shared Mesh Protection or FastSMP™ technology combines the best attributes of all the current failure recovery mechanisms into a single solution that provides the following:

- Enhanced availability: automatic multi-failure network-wide backup via network intelligence;
- Deterministic performance: sub 50ms recovery via dedicated hardware; and
- Lower capital costs and operations: shared backups via cost-effective transport layer.

While long haul transmission is rapidly moving to coherent 100 Gb/s and 500 Gb/s super-channel technology, service demands are still predominantly made up of extremely large numbers of gigabit Ethernet and 10GbE. With the move to 100G and 8 Tb/s of capacity per fiber, a single fiber cut could affect many thousands of services.

<table>
<thead>
<tr>
<th></th>
<th>Multi-failure backups</th>
<th>Fast Recovery</th>
<th>Minimal Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optical SONET/SDH: 1+1 Protection</strong></td>
<td>Single failure scenario</td>
<td>Sub 50ms recovery on fail</td>
<td>Dedicated backup resource</td>
</tr>
<tr>
<td><strong>Packet IP/MPLS: MPLS Fast Re-Route (FRR)</strong></td>
<td>Multi-failure scenarios</td>
<td>Sub 50ms for limited scenarios</td>
<td>Shared bandwidth, Packet layer $$$</td>
</tr>
<tr>
<td><strong>Digital OTN: Software Mesh Restoration</strong></td>
<td>Multi-failure scenarios</td>
<td>Up to few seconds recovery on fail</td>
<td>Shared bandwidth, Transport layer</td>
</tr>
<tr>
<td><strong>Digital OTN: FastSMP™ Hardware Shared Mesh Protection</strong></td>
<td>Multi-failure scenarios</td>
<td>Sub 50ms recovery on fail</td>
<td>Shared bandwidth, Transport layer</td>
</tr>
</tbody>
</table>

**Figure 1:** Comparison of resilience capabilities in major network technologies
The sharing of protection resources is the key to reducing total network cost, and GMPLS-based restoration is a well-known approach to achieving this sharing benefit. However, GMPLS signaling is not a lightweight protocol; it requires significant processing at each node. Also, GMPLS-based restoration is mostly a reactive approach, because the restoration resource conflict resolution is done at the time of failure. Crankbacks, in which an initial signaling attempt fails and must be repeated over a different route, are inevitable, and this can extend converge times in the network for these restoration events. To protect all of the thousands of services affected by fiber cut within 50ms using the traditional software-based GMPLS route computation approach is not scalable.

In contrast, the SMP protocol is fundamentally a proactive approach for network protection. It decouples time-critical tasks like protection activation from longer timescale GMPLS control plane route computation and convergence. The SMP protection activation protocol is designed to be lightweight, and this is a key characteristic that enables it to be implemented in hardware.

### The Importance of Hardware Acceleration

Customers often plan to use backbone transport platforms like the Infinera DTN-X for more than a decade. Hence, it was built from the ground up to handle multi-terabit scale at a highly granular service level while providing unmatched bandwidth efficiency and resilience. This philosophy drove the Infinera DTN-X to implement FastSMP™ using a dedicated hardware acceleration chip called the FastSMP™ Processor as depicted in Figure 3. Thus, protection activation is accelerated by using the more efficient SMP protocol combined with large scale hardware look up tables, designed to support 50ms recovery of thousands of services simultaneously, even in the face of multiple fiber cuts. This chip is built into every DTN-X board ever shipped. It implements a massively parallel pipelined architecture to ensure a deterministic sub-50 millisecond failure recovery end-to-end, even for networks composed of thousands of nodes, with multiple hops, and recovering from multi-terabit fiber capacity failure. The failure scenarios are handled at a highly granular level (i.e. per service) as the hardware supports tens of thousands of activation messages per second.
FastSMP™ Processor operations are completely independent of software and the GMPLS control plane. This provides not only guaranteed sub-50ms protection at enormous scale, but also provides high availability by decoupling protection activation from the control plane software. For example, FastSMP™ protection is available even when software or GMPLS is not fully functioning – such as during a software update event. In this way, innovative protection SLAs can be designed using the DTN-X platform.

**How FastSMP™ Works**

Not surprisingly, the orchestration of high numbers of service demands with a sophisticated protection hierarchy has to be supported within a powerful planning system. The first step for FastSMP™ is, therefore, to use Infinera’s Network Planning System (NPS) software to pre-calculate multi-failure scenarios, and then to populate the hardware tables contained in the FastSMP™ Processor. This is the key to ensuring the 50ms end-to-end protection capability.

Once a failure occurs, the FastSMP™ Processor will ensure protection activates in less than 50ms. At the same time, the failure notification prompts GMPLS intelligence in each node to start recalculating backup paths in real time, and then continuously updates both the hardware tables across the network and the Network Planning System if required. Thus, the three key components, NPS, the FastSMP™ Processor, and the GMPLS Control Plane, are always in sync.
Infinera is leading the way in standards development for SMP within both ITU-T and IETF, and by implementing the FastSMP™ operation in hardware, the system can ensure scalable and deterministic performance at the multi-terabit scale.

This technology may be employed in fully meshed and partially meshed transport networks, which include, but are not limited to, long-haul and metro networks. Depending on the degree of inter-connection between network nodes, SMP protection can significantly improve network resource utilization, as compared with alternative protection mechanisms.

The ITU-T is working on two documents that define shared mesh protection: G.SMP (G.808.3) and G.ODUSMP. The former protocol aims to standardize the technology-independent portions of shared mesh protection, while the latter aims to standardize it for the digital OTN layer. The protocols cover message encoding, signaling, activation and other functions necessary to achieve shared mesh protection.

Meanwhile, IETF is working on the following two drafts to standardize the application of shared mesh protection across digital circuit and packet network:

- Requirements for MPLS Shared Mesh Protection
  (draft-weingarten-mpls-smp-requirements-02.txt)
- Supporting Shared Mesh Protection in MPLS-TP Networks
  (draft-pan-shared-mesh-protection-05.txt)

Some of the functions in these protocols include defining a lightweight signaling mechanism for protection path activation.
Potential for New Revenues

As service providers move towards mesh networks and leverage technologies like FastSMP™, they have the opportunity to offer a variety of new protection tiers. Carriers in countries where multiple fiber cuts per day can be experienced are starting to examine the following different tiers:

• Premier: survivable with “hitless” performance of two network failures with highest priority;
• Elite: survivable with “hitless” performance of one network failure; best effort restoration for additional network failures;
• Protected: survivable with “hitless” performance of one network failure;
• Restorable: best effort restoration for any network failures;
• Unprotected: not survivable after a network failure, but not pre-emptible; and
• Best effort: lowest priority and pre-emptible by higher priority services.

At a minimum, FastSMP™ can provide a carrier a more competitive posture in the marketplace, enabling them to acquire and retain key customer revenue streams.

Conclusion: The Benefits of Using Infinera FastSMP™

With the interconnectedness of business operations and network reliability intersecting with an increasing number of natural and man-made threats to fiber networks, service providers need to take advantage of new protection capabilities afforded by network intelligence, hardware innovation and mesh network topologies. Infinera’s FastSMP™ solution combines the following three foundation resilience capabilities into a single technology:

• Enhanced availability: automatic multi-failure network-wide backup via network intelligence;
• Deterministic performance: sub 50ms recovery via dedicated hardware; and
• Lower capital costs and operations: shared backups via cost-effective transport layer.

Thanks to this capability, service providers can continue to offer stringent SLAs to their end-customers for protected services, and even create a hierarchy of protection classes that will provide vital service differentiation and additional revenue opportunities.