DIGITAL PROTECTION VERSUS OPTICAL PROTECTION IN REAL NETWORK IMPLEMENTATIONS

Scott Jackson, Xiaohui Yang, Emily Abbess, Benoit Kowalski, Infinera Corporation.
Email: bkowalski@infinera.com

Infinera Corporation, 140 Caspian Ct, Sunnyvale, CA 94089

Abstract: Two main protection solutions are available when protecting traffic from a cable landing station to a point of presence through a dual route backhaul. The first solution is based on optical switching, often referred to as OPTICAL sub network connection protection (O-SNCP). The second solution is based on digital switching, referred to as DIGITAL sub network connection protection (D-SNCP). Both protection solutions are designed to restore commercial services in less than 50ms. While O-SNCP is often the lowest cost implementation since it requires only a single line module or transponder at each end of the link, it suffers from operational limitations compared to the D-SCNP implementation. D-SNCP requires two line modules or transponders at each of the protection link and reacts protects much more complex failure scenarios beyond the basic Loss of Signal (LOS) that O-SNCP only supports. This paper discusses D-SNCP versus O-SNCP based on real deployments and operational experiences on commercial networks where D-SNCP eventually replaced O-SNCP deployment in order to counter traffic outages experiences with the previously-implemented O-SNCP solution.

1. INTRODUCTION

The natural mind-set to provide redundancy between the wet plant terminations and the final CLS or PoP consists of building at least two paths as diversely routed as possible between these two main elements (wet plant BMH and terminations). The next step consists of identifying the network elements that can connect those optical paths together.
Two main solutions are considered: Digital or optical.

2. O-SNCP OVERVIEW

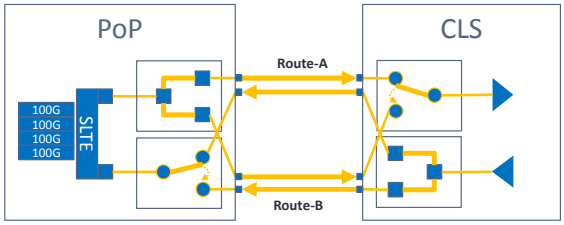

Figure-1: O-SNCP Key Elements

In the case of O-SNCP as shown in Figure-1, a transmit device splits the optical signal into two or more outputs on the transmit direction. Each output is connected to the optical fibre corresponding to a specific optical route. At the end of the link, a receiving device will select the optical path that is working properly. The receiving device or optical switch will typically be connected to the preferred optical path (usually the shorted path for latency consideration). Should this optical path fail due to a fibre cut, the receiving device will simply detect the loss of optical signal (LOS) and switch immediately to an alternate path that will be expected to be up and running. The receiving device is usually not monitoring the health of the alternative protection paths for suitability in the event of an LOS. If the alternative protection paths are sufficiently diversely routed this is a safe assumption. These solutions are symmetrical between the

protection endpoints. The device providing the optical protection is therefore always composed of two major components: an optical splitting mechanism in the transmit direction and an optical switch in the receive direction.

3. O-SNCP BENEFITS

This protection mechanism as several benefits. The first benefit is the speed of switching. Typically less than 50 milliseconds (50ms), an optical protection device is the fastest protection mechanism in the optical Telecom industry. This speed is achieved because no communication protocol is necessary between the two end points (CLS & PoP). The switching decision is done on the receive end without need for communicating to the far end; an optical fault was detected and a protection switch took place as a result. The second benefit of O-SNCP is the simplicity of the implementation and involved devices. A single optical switch can be implemented to provide protection to the whole of the WDM signal. Terabits of capacity can be protected with a single network element per end site. As a direct consequence of this minimal hardware implementation is a very important factor: optical switch element is inexpensive. Optical protection is overall a simple, low-cost, and efficient way to provide backhaul protection.

4. O-SNCP LIMITATIONS

O-SNCP nonetheless suffers from its simplicity. It only switch when there is a clear cut leading to a clear loss of signal (LOS). Any other fault will not cause the receive end to trigger an optical switch from the active path to the protection path. Especially relevant in the case of the 100G coherent technology, the actual end to end restoration time may be much higher compared to the expected 50ms. Some 100G transponder implementations requires several seconds for the transponder to lock its local clock with the incoming signal phase in order to recover and process the phase modulation. During the switching time, the receive end of the 100G transponder will lose this phase lock and therefore will start a reacquisition phase that can take several hundreds of milliseconds. More recent 100G transponder implementations have mechanisms to avoid this long reacquisition time but this feature is vendor specific. Because of its mode of operation, O-SNCP can produce undesirable system-level results in what otherwise seem practical designs.

5. D-SNCP OVERVIEW

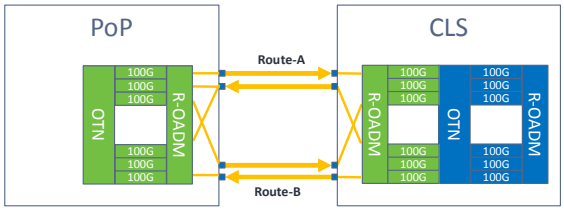

Figure-2: D-SNCP Key Elements

In the case of the digital approach D-SNCP, the optical signal is not split into multiple routes as shown in Figure-2. Each redundant path is equipped with its own set of transponders. In the case of the most advanced implementations, GMPLS-based handshakes are continuously taking place on each individual diverse path between facing transponders. In other words, one transponder at one end of the link directly communicates through GMPLS Protocols with its counterpart at the other end of the link. Depending on the vendor technology, each individual service can be protected, restorable, or unprotected. In the case of a cable cut, the GMPLS handshakes on the affected optical path will stop and the end systems will automatically re-route the affected services on alternative paths based on their level of protection. The protected services have reserved protection routes,

thereby providing switching times guaranteed at less than 50ms. The restorable services will take second priority and the end devices will compute a new active route for these service types. The unprotected services will be down as expected. In contrast to the optical protection implementation, the digital protection requires a more complex end device. The incoming signal from the wet plant is converted to a digital signal and each service is tagged to the level of required protection. Each service transits through an OTN switching fabric that provides the link between the wet plant termination and the backhaul routes. The services are then multiplexed and groomed into optical carriers that are multiplexed on to the backhaul routes. OTN cross-connect terminals today [1], like SDH/SONET cross connect terminals in a recent past, are used to perform digital protection schemes.

6. D-SNCP BENEFITS

When the optical signal is converted into a digital stream, which is in turn converted to services, it is possible to access to a large range of information that allows a much richer level of fault diagnosis. Where optical switching will switch on LOS only, digital switching will be triggered based on client-side faults such as LOS, Signal Defect (SD), Loss of Frame (LOF), Alarm Indication Signal (AIS), Loss of Acquisition (LOA), LF, Loss of Synchronization (LOSYNC)[3]. Those failures are detected on the transponder level on the terminals. They are complemented by alarms that could be generated by other network elements on the optical path like mux/demux units or in-line terrestrial amplifiers. As the decision is decided at the digital level, a much wider range of events can trigger a protection switching. Another benefit of digital protection implementations is the broadening of protection level of service possibilities. When optical protection cannot differentiate between services and thus operates on the entire WDM signal (Multiplex Section switching only), digital protection can operate at each individual service level. This opens the door to multiple types of service offerings as well as better bandwidth utilization of the available infrastructure since protection bandwidth can be used for pre-emptable services, for instance. Finally, because of the constant GMPLS-based handshake, there is no issue with losing the phase of the incoming signal.

7. D-SNCP LIMITATIONS

The main drawback of digital protection can be its cost, and this is the main argument against it. However the cost depends entirely on how digital protection is implemented and how efficient the optical-digital conversion is achieved. Photonic Integration has been demonstrated as an extremely efficient way to achieve cost effective digital protection. The cost of the digital protection has to also be considered relative to overall system (wet plant and dry plant) cost and features, as D-SNCP can have a very large impact on the customer perception of system-level service quality. The sub-50ms protection is proven to bring significant benefits on IP layers in term of network stability even if IP routers can also implement some fast and robust protection mechanisms.

8. REAL NETWORK IMPLEMENTATIONS

The digital protection implementation has recently shown its benefits on existing backhauls networks, which used to operate with the optical protection implementation. Originally considered as a cost effective and efficient implementation, the optical

protection was proven in reality inefficient when confronted to the realities of the field. Even though O-SNCP operated correctly, the experience was so disappointing and the cost saving so negligible relative to customer dissatisfaction, sales loses and customer compensations, that those networks were migrated to digital protection. The main argument against optical protection in those specific backhauls was that it was not working. In the real world, it is not always possible to test properly a fault repair and measure adequately the efficiency of an optical splice. Contrary to a lab environment where all the required equipment is available, it is not always possible to have an OTDRs or other sophisticated equipment available at each end of a faulty span. Faults typically happened in those backhauls in areas which were difficult of access. Although the fault diagnosis was quick and usually very accurate, getting to the fault location was arduous. Splicing devices have to be carried in backpacks causing calibration of the devices to be questionable. Once the optical cut was repaired, the optical protection implementation would not allow the operational engineers to see if the repair was effective and to test the losses of the splicing was meeting the requirements. The issue was usually found after an optical protection switch from the active path to the repair path. At that time, the previously active path was down and the protection path was not useable. It was then a race to repair the most easily accessible failure location. The 50ms promise was reduced to several hours of outage. This simple situation would never happened in the case of the digital protection where the GMPL-based handshake would have started immediately after the completion of the splicing. In seconds NOC engineers would have been able to confirm the health of the link and the efficiency of the repair. Alternatively the necessary pre-emptive actions could have been planned in a controlled manner should additional intervention was required. This would have led to being certain the route was able to carry efficiently traffic when required. This live monitoring capability is key, especially in locations where backhaul cuts are commonplace.

9. CONCLUSION

In conclusion, this article shows the inherent superiority of digital protection over optical protection due to more expansive triggering mechanisms, fast protection delivering higher service availability, opportunities for expanded service levels, and potential for more efficient bandwidth utilization. D-SNCP has demonstrated availability superiority cost-effectiveness in live deployments, where O-SNCP was ineffective and customers were adversely affected.

10. REFERENCES

[1] International Telecommunications Union (ITU) Optical Transport Network G.709
[2] International Telecommunications Union (ITU) Synchronous Digital Hierarchy (SDH) G.783
[3] International Telecommunications Union (ITU) Transmission Protection G.841