Shared Mesh Protection (SMP): What It Is and Where It Fits

SMP protection switching is faster than restoration based on ASON/GMPS protocols and can reduce network costs.

Introduction

For the world's complex infrastructure of information and communications technologies, industry standards are critical to the interoperability of all networks regardless of whether they are for voice, data or video. Industry standards allow these networks to "speak the same language," and be able to exchange information among them. The Study Groups of the International Telecommunication Union – Telecommunications Sector (ITU-T) assemble groups of industry experts and scientists from around the world to work on and develop these standards, providing guidance for the industry to follow. By voluntarily complying with these standards, companies can avoid costly proprietary technologies and designs.

The ITU-T is currently working on standards related for protection of connections and services in mesh networks, called Shared Mesh Protection (SMP). To understand these standards, it is helpful to understand the context of these standards and how they fit in the eco-system that is the modern telecommunications network.

This paper provides the background and context for the current work on shared mesh protection, drilling down the place of ODU-level shared mesh protection standards, and explains the relevance for Xtera.

The ITU-T

"The ITU was founded in 1865 as the International Telegraph Union. It took its present name in 1932, and in 1947 became a specialized agency of the United Nations" (http://www.itu.int/en/about/Pages/history.aspx). The ITU is based in Geneva, Switzerland, where it has office facilities for full and part-time staff, and extensive conference facilities utilized by meetings year round. The ITU-T is driven by contributions and has a consensus-based approach. That means member states and companies submit contributions with proposals related to new or existing standards. The contributions are presented and discussed at face-to-face meetings, via e-mail, or other electronic media. Decisions are reached and actions taken on those decisions if/when consensus is reached on a course of action. Countries and companies have equal rights to affect the formation of standards, which are called Recommendations. Per the name, Recommendations, adherence to the standards is entirely voluntary and that compliance is not verified or certified by the ITU-T itself. The ITU-T is the world's only, truly global, telecommunications standards development organization today.

Standardization work is carried out by the technical Study Groups (SGs) in which representatives of the ITU-T membership develop Recommendations (standards) for the various fields of international telecommunications. The Study Groups for the 2013-2016 Study Period are:

SG2	Operational aspects
SG3	Economic and policy issues
SG5	Environment and climate change
SG9	Broadband cable and TV
SG11	Protocols and test specifications
SG12	Performance, QoS and QoE
SG13	Future networks (& cloud)
SG15	Transport, access and home
SG16	Multimedia
SG17	Security

Detailed descriptions of these Study Groups can be found at the ITU-T web site (http://www.itu.int/en/ITU-T/Pages/default.aspx).

Study Group 15 – Networks, Technologies and Infrastructures for Transport, Access and Home

Xtera is a member of Study Group 15 (SG15). SG15 deals with "Network, Technologies and Infrastructure for Transport, Access and Home" (http://www.itu.int/en/ITU-T/studygroups/2013-2016/Pages/default.aspx). The Recommendations produced by SG15 are detailed technical specifications dealing with technologies and architectures of optical transport networks. They enable long-haul global information exchange, and fiber- or copper-based access networks through which subscribers connect. While SG15 also deals with standards for home networks and may cover other areas related telecommunications, Xtera has only minor involvement with those parts of the SG15 standardization process at this time.

SG15 is organized in three Working Parties (WPs). There are various Questions (Qs) within each Working Party. The Working Parties and Questions in Study Group 15 are:

WP1/15 Transport aspects of access, home and smart grid networks

Q1/15	Coordination of access and home Network Transport standards
Q2/15	Optical systems for fiber access networks
Q4/15	Broadband access over metallic conductors
Q15/15	Communications for Smart Grid
Q18/15	Broadband in-premises networking

WP2/15 Optical technologies and physical infrastructures

Q5/15	Characteristics and test methods of optical fibers and cables
Q6/15	Characteristics of optical systems for terrestrial transport networks
Q7/15	Characteristics of optical components and subsystems
Q8/15	Characteristics of optical fiber submarine cable systems

Q16/15 Outside plant and related indoor installation
Q17/15 Maintenance and operation of optical fiber cable networks

WP3/15 Transport network characteristics

Q3/15 General characteristics of transport networks
Q9/15 Transport network protection/restoration
Q10/15 Interfaces, Interworking, OAM and equipment specifications for packet-based transport networks
Q11/15 Signal structures, interfaces, equipment functions, and interworking for transport networks
Q12/15 Transport network architectures
Q13/15 Network synchronization and time distribution performance
Q14/15 Management and control of transport systems and equipment

Xtera is actively involved in Q5/15, Q6/15, Q8/15, Q9/15, Q11/15, Q12/15 and Q13/15. Dr. Mark Jones of Xtera is the current Rapporteur (chairman) of Q11/15.

Question 9/15 – Transport Network Protection / Restoration

With the rapid growth of network traffic and the development of very high bit rate transport systems, it is Xtera's belief that the development of network protection and restoration standards will be a critical aspect of the next generation of standards. While there is already a set of standards defined for different types of networks, the development of the shared mesh protection is of special interest to Xtera. One of the main benefits for shared mesh network protection is the ability to reduce cost by sharing protection and restoration resources. It is also specifically designed for mesh type networks, which continues to increase in popularity among carriers worldwide. Q9/15 is responsible for the development of the shared mesh protection and the associated technology specific Recommendations, such as the Recommendation for shared mesh network protection at the Optical Transport Network (OTN, based on ITU-T Recommendation G.709 interfaces) Optical Data Unit (ODU) granularity (ODUSMP).

Recommendation ITU-T G.808.3 – Generic Protection Switching – Shared Mesh Protection

G.808.3 Scope

The current Q9/15 work on shared mesh protection is based on ITU-T Recommendation G.808.3 "Generic protection switching – Shared mesh protection" (http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11788). It has the following scope.

This Recommendation defines the architecture framework of a generic Shared Mesh Protection (SMP) mechanism. The SMP is designed for a connection-oriented network and is not dependent on the presence of a control plane. The primary feature of this path-based procedure is the use of pre-computed and pre-allocated resources for protection and restoration. In SMP, the protection resources can be shared among two or more protection transport entities. Only one of these protection transport entities can use the shared protection resources at any one time. Recommendation ITU-T G.808.3 covers only the generic procedure of the shared mesh protection. Technology-specific shared mesh protection procedures are expected to be defined by other technology-specific Recommendation(s).

What is a Meshed Network?

Based on the ITU-T definition, “A meshed transport network is one in which each node in the network is interconnected by at least two links whose remote ends are on different nodes from each other”. Figure 1 shows an example of such a network.

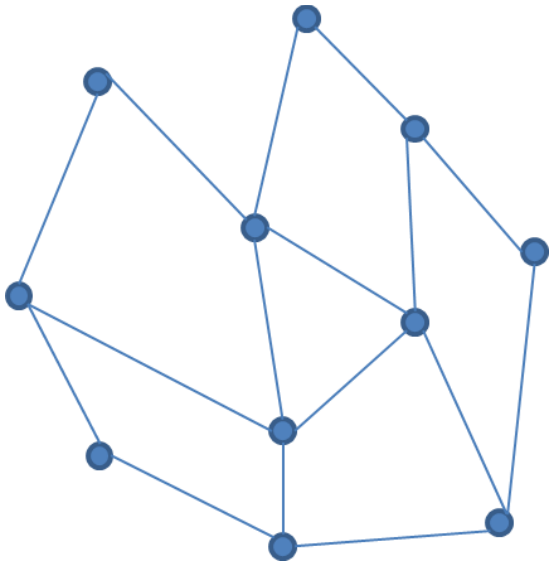

Figure 1: Example of a meshed network.

In some cases, the overall transport network may contain nodes that are not connected to the meshed network. Figure 2 shows the example of such a network. In this case, nodes that are not connected would not be considered as part of the meshed transport network. The process of SMP will therefore not be applied to those nodes.

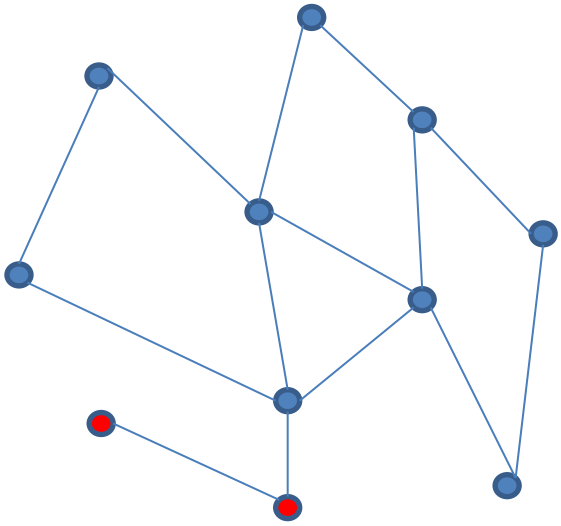

Figure 2: Example of a network with a partial meshed configuration.

A fully-meshed topology is one in which each node is directly connected to every other node in a network. Figure 3 shows an example of such a network.

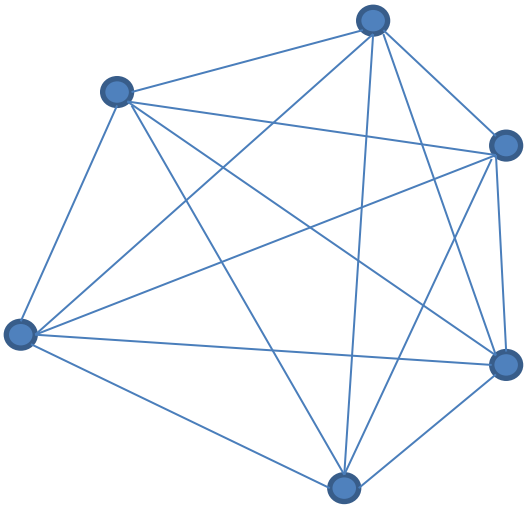

Figure 3: An example of a fully-meshed network.

Fully-meshed network topologies offer the highest degree of survivability in the event of failures. They also require the largest number of paths to complete. Therefore, they are the most costly to build. Consequently, most meshed transport networks are only partially meshed, requiring traversing intermediate nodes to connect between two end nodes.

Reduction of Protection Resources

Traditionally, networks are protected using either 1 for 1 (1:1) or 1 for N (1:N) schemes. As the capacity of the network paths increases, equipment associated with these paths and their protection routes becomes expensive. Reserved dedicated capacity for protection cannot be used for revenue generating traffic and therefore increases the overall cost structure of the network. Sharing of protection resources in meshed network architecture allows for reduction of network costs by eliminating dedicated protection resources. Such architectures may also be designed to provide the level of "guaranteed protection" and capacity efficiency desired by the service providers.

SMP Architecture Types – Overview

SMP may be employed in fully-meshed and partially-meshed core and metro transport networks. An SMP architecture involves multiple normal traffic signals, where each signal is associated with a working transport path and one or more protection transport paths. SMP architecture is based upon m:1 protection (where m may be greater than or equal to one).

In an m:1 SMP architecture, each working path is protected by m protection path(s). In this architecture, the working transport path can be protected when one of the m protection paths is available. Figure 4 shows an example of a simple m:1 SMP architecture.

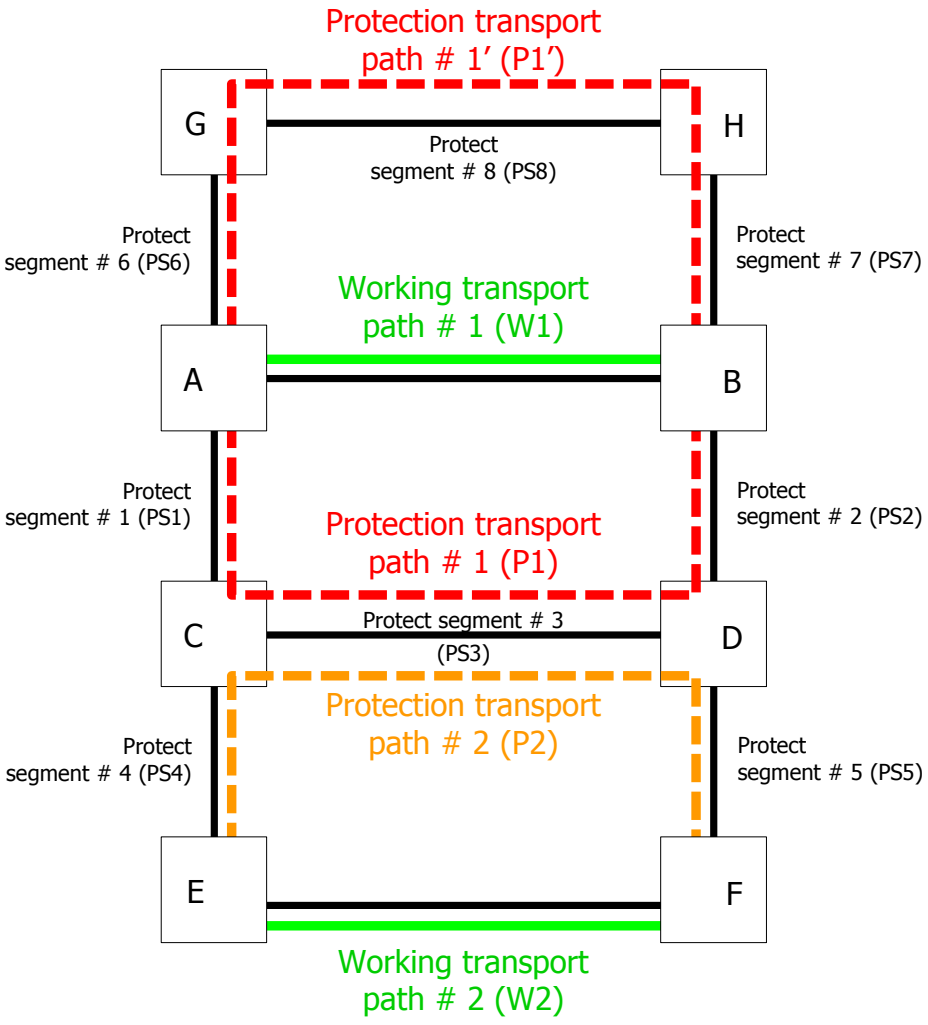

Figure 4: Example of a m:1 SMP architecture.

There are two working transport paths, which are W1 (A-B) and W2 (E-F) highlighted in green color in Figure 4. The protection transport paths in this example have been pre-configured as follows:

- For W1, there are two protection transport paths: P1 (A-C-D-B) and P1' (A-G-H-B); these protection transport paths are highlighted in red color in Figure 4;
- For W2, there is one protection transport path: P2 (E-C-D-F), highlighted in orange color.

If a failure of W2 is detected, the corresponding protection transport path P2 will be activated to carry the traffic. As a result, the protection segment PS3 will be fully occupied by P2. In this case, the protect path P1 can no longer be used to protect the working path W1. But the other protection transport entity P1' can be used to protect the working transport entity W1 in case of a simultaneous failure with W1 and W2. Therefore for the example of W1, m is equal to 2.

SMP for Circuit Networks

SMP can be used for both the circuit switch network, such as a SDH/OTN network, and a packet network. The process of applying SMP to these networks will be different. In circuit switch networks, the cross-connects in the intermediate nodes of the protection transport path cannot be pre-established when the protection segment is shared by multiple protection transport paths. In this case, the intermediate nodes need to establish the cross-connects for the protection transport path when the protected working transport fails.

The end points of each working transport path will have the monitoring functions to monitor the status of the working path. The detected Signal Fail / Signal Degrade (SF/SD) status will trigger the protection switch procedure. Meanwhile, the nodes along the protection transport entity should also have the monitoring functions to monitor the status of the resources of each protection segment. If any of these protection segments are not functioning, the monitoring function will prevent the transfer of traffic into any of these failed segments.

SMP for Packet Networks

In packet-switched networks, it is possible to pre-establish different protection transport paths sharing the same bandwidth of the shared protection segment. In normal conditions, in which normal traffic signals are transported via working transport paths, only Automatic Protection Switching (APS) and Operation, Administration, and Management (OAM) packets are transported via protection transport entities. The bandwidth of a shared protection segment should be allocated in such a way that it may be possible to protect any of the working transport paths whose protection transport paths are sharing the protection segment.

The end points of each working transport paths will also have the monitoring functions to monitor the status of the working transport paths. The detected SF/SD status will trigger the protection switch procedure. Because the protection transport entity is pre-established, the status of the protection transport path can also be monitored at the end points.

Other Supported Functions

The Recommendation ITU-T G.808.3 also specifies the standards on many related requirements. Requirements such as switching types, operations types, pre-emption procedures, and path status monitoring are included.

There are several important topics, such as Automatic Protection Switching (APS) protocol and automatic switch, that are under further study and the detailed requirements will be included in future versions of the Recommendations.

ODU-Specific SMP Application

From the onset of developing the Recommendations for the shared mesh protection, the group of experts working on the project agreed that the initial Recommendation

should only provide generic guidelines for the shared mesh protection process.

Recommendations for mesh networks employing specific technologies would be developed in separate projects using the standards developed under Recommendation ITU-T G.808.3 as a basis. The first such technology-specific project is for Optical Transport Network (OTN) protection switching using the shared mesh protection principles.

Scope of Draft Recommendation G.ODUSMP

The intended scope of draft Recommendation G.ODUSMP is to define the protection switching and related protocols for shared mesh protection at the Optical Data Unit (ODU) level (ODUSMP). It operates on either the end-to-end ODU path or ODU tandem connection. The ODUSMP procedure will be based on the approved generic shared mesh protection architecture as defined in G.808.3.

The intended procedure will again use pre-computed protection paths that are pre-configured into the network. These protection paths will be activated when a failure in the network is detected via data plane protocol operations.

The work for this Recommendation will focus on the activation of the protection paths, and the information the network elements must maintain to support the activation of protection paths.

Current Status of ODUSMP

A group of Q9/15 experts are currently hard at work on this draft Recommendation. A list of topics/issues was compiled at the September 2013 interim meeting, and work on solving those issues will continue at the next ITU-T meeting scheduled for March 2014. Xtera is an integral part of this group and will continue to work with the experts in this area for the completion of this Recommendation.

Some of the Issues and Work Topics for ODUSMP

Since the current ODUSMP protocol is designed to modify the multiplex structure of the server trail as part of the activation process, there is a need to also decide on the protocol for configuring the multiplex structure and the activation path. There have been a lot of discussions on whether separate protocol stages will be needed to activate a protection path and to configure the multiplex structure of a server layer link.

Another key issue is the resource availability notifications from intermediate points to end points. The speed of such notification can impact the performance of the ODUSMP protection switching and therefore be critical. The intention of such notification process is to help the endpoints make better and faster decisions in multiple path scenarios by not attempting to activate protection paths that are not available for protection. The ODUSMP interest group in Q9/15 is in the process of analyzing several scenarios and is working hard to reach consensus on the requirements.

There are other open issues that must also be resolved prior to the submission of the proposed standard for approval. Some of those issues are captured in the following questions:

1. How would the ODUSMP protection scheme scale for larger mesh networks?
2. How would it work in future high bit rate networks containing circuits beyond 100G?
3. How will the protocol deal with the frequent updating of the ODU data bases?
4. How will it handle both single circuit failure scenarios and multiple circuit failure scenarios?

The completion of this standard may be several months or years away. Xtera is working closely with other industry experts in this area for solutions to the open issues.

Conclusion

The concept of shared mesh protection is important for service providers as it could help to reduce network costs and also allow the service providers to market services with different grades of protection. For example, mission critical circuits could be pre-configured to have the best protection scheme while the other circuits could be pre-configured with a much more cost effective architecture. Network operators are requesting that the ODUSMP protocol be simple to implement and be effective in all cases. One thing is clear, however, the development of a Recommendation to standardize ODU level shared mesh protection could prove to be particularly important as more and more networks utilize OTN switches (using ODU switching fabrics).

Note: In another white paper, entitled “Relationship between SMP, ASON, GMPLS and SDN”, Xtera discusses the relationships and differences between the SMP, ASON, GMPLS and SDN architectures and protocols.

Maximizing Network Capacity, Reach and Value

Over land, under sea, worldwide

Edition Date: February 2014

Version: 1.0