ONTC PRISM Newsletter

Dear ONTC Members,

A warm welcome from the Editorial desk of the ONTC's newsletter "Prism". It is our pleasure to bring to you this fourth edition of PRISM – ONTC's quarterly newsletter.

The current issue focuses on a wide variety of subjects – from covering Stanford University's Photonics and Networking Research laboratory, to the industry work in 802.1 as well as MPLS-TP to the emerging work in time-synchronization and service protection in Ethernet switched networks.

ONTC will meet soon at OFC – which will be held in downtown Los Angeles (March 6-10). Subsequent to OFC, the IEEE 802 Standards' Plenary will be held this year in Singapore. ONTC sponsored conferences are doing very well – the recently concluded IEEE ANTS 2010 held in Mumbai drew about 300 folks – most of whom were from the industry.

In this issue of Prism we bring to you 4 articles on a wide range of topics.

The first article is by the Photonics and Networking Research Laboratory at Stanford University. It is titled, "The Next-Generation Optical Access Network at Stanford Photonics and Networking Research Laboratory". This laboratory is well known for its cutting edge research in photonic networks. The article describes the state of the lab, the projects being undertaken and the developed technology. Specific focus on hybrid networks and energy efficiency are discussed.

The second article is by Monique Morrow from Cisco Systems Switzerland (and also a TAB member with Prism). Monique gives an update MPLS-TP (Multi-Protocol Label Switched – Transport Profile) community. Much is happening in that community and this article describes some of the latest developments.

The third article is titled, "Ethernet Support for Time Synchronization Protocols (IEEE P802.3bf)," and is authored by Marek Hajduczenia, Henrique J. A. da Silva Steve Carlson and David Law. The authors – all of whom are veterans of the standardization community do a great job in describing the technolgy contribution within time-synchronization in Ethernet networks. They specifically describe the proposed 802.3bf draft as an important mechanism for time synchronization in Ethernet networks. This technology is very important for applications such as mobile backhaul.

The fourth article is by Zehavit Alon who focusses on Ethernet Service Protection using External Intefaces. The article talks about possible standardization in this space using a novel protection mechanism for Ethernet services.

From the editorial desk, we are encouraging you to submit your work to this newsletter. The newsletter aims at achieving timely publication of your work after a peer-review process. TAB members are working hard to enable work to see the light of the day and are also helping prospective authors in fine-tuning their manuscripts.

As you are aware the editorial desk does highlight events, call for papers and new standards work – all of which would be relevant information for our readers. So please do send in any such information that you would like to see online for the next issue of Prism!

We also do hope readers would send in their thoughts on how to make Prism better – we would be happy to publish their messages even if all of these cannot be adopted at the same time!

We invite prospective authors send articles of up to 4 pages (single column, 10 point font, with all one-inch margins) to submissions@ontc-prism.org. The deadline for reception of articles is April 1, 2011 for the next issue of Prism.

On behalf of the TAB we are thankful to the IEEE Communication Society as well as to the ONTC officers Byrav, Suresh, Admela and Dominic who have supported us in making this newsletter happen.

It is our hope that the newsletter would bring the community together and identifying areas of growth and common interest.

Ashwin Gumaste, IIT Bombay.

Message Board

Standardization:

IEEE SIEPON		http://grouper.ieee.org/groups/1904/1/
IEEE Interim Meeting (802)	Sept 13-16, York, UK	http://www.ieee802.org/1/meetings/index.html#sep10gen
IETF	Nov 7-11, Beiging, China	http://www.ietf.org/meeting/79/index.html
IEEE Plenary	Nov 7-11, Dallas, USA	http://ieee802.facetoface-events.com/future
ITU SG15	Oct 18-22	http://www.itu.int/ITU-T/studygroups/com15/index.asp

Academic Conferences

IEEE/OSA OFC 2011	March 6-10. Los Angeles	http://www.ofcnfoec.org/
IEEE Globecom 2010	CFP March 31 Conf Dec 6-10. Miami	http://www.ieee-globecom.org/
IEEE LCN 2010	CFP April 12. Conf Oct 11-14 Denver, CO.	http://www.ieeelcn.org/
IEEE ICC 2011	CFP Sept. 7: June 5-9, 2011, Kyoto, Japan.	http://www.comsoc.org/confs/icc/2011/index.php
IEEE ANTS 2010	CFP July 15: Conf: Dec 15-17, Bombay, India	www.ieee-ants.org
Infocom 2011	Conf April 10-15, Shanghai, China.	http://www.ieee-infocom.org/2011/
IEE Globecom 2011	Houston TX	www.ieee-globecom.com

The next ONTC meeting would also be held in Miami, during IEEE Globecom.

We would be happy to include more conferences in the above list, if readers email editor@ontc-prism.org a CFP of the conference. The conference must be at least technically supported by ONTC or ComSoc to be included in the list above and follow the ONTC endorsement policy.

Key journals reporting results in the optical networking area:

IEEE/OSA Journal of Optical Communication and networks (JOCN)
http://www.opticsinfobase.org/jocn/journal/jon/author.cfm
IEEE/OSA Journal of Lightwave Technology: http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=50
IEEE/ACM Transactions on Networking: http://www.ton.seas.upenn.edu/
IEEE Communications Magazine: http://mc.manuscriptcentral.com/commag-ieee
IEEE Network: http://dl.comsoc.org/ni/

The Next-Generation Optical Access Network at Stanford Photonics and Networking Research Laboratory

L. G. Kazovsky[+], S.-W. Wong, S.-H. Yen, J.-Y Kim and M.R.N. Ribeiro[*]
Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA
**Department of Electrical Engineering, Federal University of Espirito Santo, Brazil*
+Corresponding Author:l.kazovsky@stanford.edu

1. Introduction

The improvement in the performance of personal computers and consumer electronic devices has made possible expanding demands of bandwidth consuming multimedia services, such as video on demand and video conferencing. As a result, the next-generation optical access (NGA) networks have to evolve to higher bit rates over wavelength division multiplexing (WDM) systems with more sophisticated medium access control (MAC) to address those and new demands for services that will require even higher throughputs [1]. In addition to client's needs, service providers will require from NGA architectures other features such as flexible deployment and easy upgradability to serve even more users by longer reach (over 100km) equipment. There are also the challenge of devising more dependable network topologies for these long-reach NGA schemes. However, the profit margin per bandwidth delivered to customers is being reduced by intense competition, so that new concepts that enable to reach more clients with the lowest possible cost will be required by network operators and service providers. Therefore, the NGA network with affordable and reliable architectures, that really fulfill the future needs of end users, will depend on the efforts to bridge the gap between the creative, but sometimes uncompromising, solutions proposed by academia and the cost and reliability restrictions of vendors and network operators.

This newsletter presents the proposals for the NGA networks that are currently being investigated by Stanford photonics and networking research laboratory (PNRL). Section 2 brings a brief description of a hybrid (optical-wireless) network architecture that is able create a more scalable topology when combining passive optical networks (PON) with wireless mesh networks. Provided that the efficient use of energy is a must in any future network scenario, Section 3 introduces the contributions of PNRL to this important topic. In order to provide ubiquitous, blanketed broadband access service in metropolitan area, the NGA networks can no longer rely on today's tree-based PON due to its single point of failure limitation. Section 4 presents the PNRL views on why reliability (and also security) issues have to be taken into account as the long-reach topological approaches will emerge in NGA networks.

2. Hybrid Networks

Optical network technology was initially developed for long-distance and high-bandwidth communications, while wireless network technology for the purpose of short-distance communication systems that do not require high bandwidth but do require flexibility. For ubiquitous Internet access, optical and wireless communication technologies have been employed in last-mile connections to enhance bandwidth and to enable flexibility and mobility, respectively. Today it is clear the need for convergence of optical and wireless technologies at the access segment of the Internet hierarchy, as illustrated by Fig.1. A hybrid optical and wireless access network would combine high optical capacity and flexible wireless deployment that is economic and scalable.

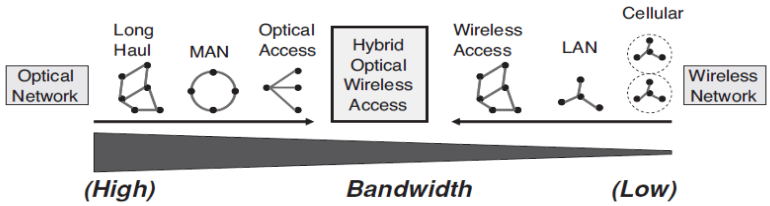

Fig. 1. Relationships between bandwidth availability and typical topologies for both optical to wireless networks [1].

PNRL has investigated the Grid Reconfigurable Optical and Wireless Network (GROW-Net). GROW-Net utilizes dark, urban optical grid network to provide the essential bandwidth capacity while efficiently leveraging the flexibility and economic advantage in the wireless mesh network. A reconfigurable optical backhaul aims to address

the scalability issue in wireless metropolitan networks (WMN) and upgrade for hierarchical wireless access networks. In this approach, time-division multiplexing (TDM) PON technology is leveraged due to its scalable MAC, flexible architecture, cost-effectiveness, and technological maturity. Reconfigurability is implemented in the optical backhaul for bandwidth reallocation to improve resource utilization. A experimental test-bed has already demonstrated its feasibility. An integrated routing algorithm has been developed for this hybrid architecture. This algorithm takes advantage of the optical backhaul to collect a real-time loading situation and network conditions and then locate the optimum ONU/gateway and route in a WMN. Simulation results have shown that throughput and delay improvement result from load balancing among multiple gateways [1].

3. Power Efficiency

A significant amount of energy is expected to be consumed by the access segment of the network in the future. The importance of conserving energy in fixed access networks has been witnessed by the setup of the IEEE P802.3az Energy Efficient Ethernet task force and recent activities in ITU-T study group 15. In particular, study groups for the TDM-PON standards including IEEE Ethernet PON (EPON) and ITU-T Gigabit-capable PON (GPON) are recently investigating options to introduce sleep mode or doze mode optical network unit (ONU) to reduce energy consumption.

It has been experimentally demonstrated by the PNRL team a sleep mode ONU architecture that enables ONU to transition from sleep mode to active mode in less than 64ns using fast clock and data recovery (CDR) circuit and a novel just-in-time sleep control (JIT-SC) scheme over a 2.5 Gb/s (downstream)-1.25 Gb/s (upstream) testbed. JIT-SC leverages existing dynamic bandwidth allocation (DBA) control sequence and messages to minimize overhead and modifications to existing networks [2].

There is still room for improvements in energy efficiency issues on the optical side of the network as well. In current optical access networks, a passive power splitter is employed in the field and power is equally distributed among users. This presents a waste of energy, since all connections, including unused and nearby connections, receive the same amount of power, whether they use it or not.

In order to insert intelligence into an access network for better optical power distribution among end users, passive components could be replaced with power-hungry active components. In the PNRL view, however, the adaptive mechanism should not come at the cost of sacrificing energy efficiency. A better solution for next generation PON network is the use of components with multiple splitting ratios that should require power only during network reconfiguration. In other words, a Quasi-PAssive Reconfigurable (QPAR) device. If the system wants to change the optical power distribution, the remote office will sends a certain amount optical power to the photovoltaic cell and change it. Once the reconfiguration mechanism has reached the desired system state, it latches into place and is able to maintain its state without consuming power. By making the system latchable, flexibility is achieved but the need for energy consumption for holding the networks to a given configuration is eliminated [3].

3. Towards More Dependable Architectures

Currently deployed TDM-PON networks are based on a tree topology, with a feeder fiber, a splitter at the remote node, and distribution fibers to each customer. Basically, protection of access network is usually performed by duplicating fibers or equipments to be protected. Full protection of access network could be easily accomplished by fully duplicating whole network elements. However, these kinds of naive approach would significantly increase cost of deployment such as capital expenditure (CAPEX). Therefore, economically meaningful deployment cost should be considered as well.

Future approaches must consider fault-tolerant architectures to minimize various failure impacts on access networks. In the long term, PNRL is working with the perspective that the access topology can go from multiple trees to a ring topology, which can cover even metropolitan geographical areas. Ring topologies are sometimes a more cost-efficient way to provide service to many users with less infrastructure. The feeder fiber, in this case, can be shared among many more users than in a tree topology. In developed markets, even though this would require a higher investment in deploying the extra fiber required for the ring, that approach allows for greater resource sharing and alternative paths for protection and restoration.

The Deutsche Telekom/Stanford Next Generation Access Network (DAN) project addresses those issues. The proposed topologies for NGA networks in DAN are shown in Fig. 2. Iin the architecture 1, there is the tree topology

to reach the optical network unit (ONU), but note that the central office stands in the center of the ring and it is connected to the ring via multiples points improving the overall reliability. The use of a combination of WDM and TDM add flexibility to enabling operators to match diverse dynamics fluctuations of traffic demand. However, in the Architecture 2 the central office is connected to the external ring via reconfigurable switches (e.g., QPAR elements). This will enable network operators higher degree of freedom for providing restoration, protection and dynamic topological reconfigurations in order to better accommodate the traffic between the central office and the diverse ONUs [3,4].

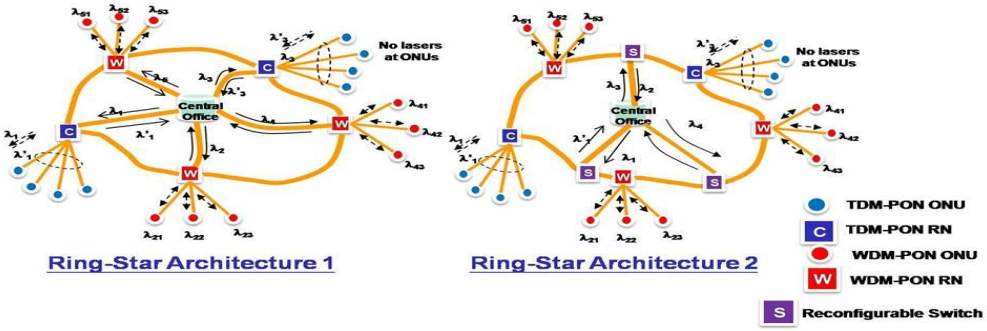

Fig. 2. NGA architectures in the DAN project.

The current research into dependable networks at PNRL is assessing the impact of service interruption caused by fiber cuts, and those caused by equipment malfunctioning as well. This includes optical line terminal (OLT) and ONU failures and other NGA equipments in the distribution network. Their failure modes and the resulting impacts must be quantified. Malicious attacks should be another concern. As thousands of customers might be served by these long-reach NGA networks, there must be mechanisms for preventing disruptive attacks. Moreover, it will require techniques for tracing back malfunctioning nodes as well as malicious behavior. PNRL has proposed and experimentally investigated a few solutions to these problems [5].

4. Summary

PNRL team demonstrated that wireless-fiber is a practical solution to addressing the challenges encountered by different solutions in the last-mile connection infrastructures. PNRL has also addressed the energy efficiency issue with proposals for both fast wake-up capability and adaptive power distribution with QPAR network elements. Topological issues for long-reach PONs are also under investigation, as well as security and accountability aspects for the NGA networks. There are further challenges ahead in devising new enabling device for NGA, new modulation schemes associated to more advanced MAC and DBA, and integrated routing algorithms taking into account quality of service constraints, resilience and differentiated protection polices.

5. Acknowledgments

The authors are thankful to the NSF (Award Number 0627085) for funding the GROWNet Project, Deutsche Telekom for the financial support and for the valuable inputs and insights to the DAN Project, and CAPES (Grant 1176-10-2) for funding the visit of Prof. Ribeiro.

6. References

[1] L. G. Kazovsky, N. Cheng, W.-T. Shaw, D. Gutierrez, and S.-W. Wong, "Broadband Optical Access Networks: Emerging Technologies and Optical-Wireless Convergence, John Wiley & Sons Press (2011).

[2] S. Wong, S. Yen, P. Afshar, S. Yamashita, and L. G. Kazovsky, "Demonstration of Energy Conserving TDM-PON with Sleep Mode ONU Using Fast Clock Recovery Circuit," in *Optical Fiber Communication Conference*, OSA, 2010.

[3] S.-H. Yen, S.-W. Wong, S. Das, Ning Cheng, Jinwoo Cho, S. Yamashita, O. Solgaard, L.G. Kazovsky, "Photonic components for future fiber access networks," IEEE Journal on Selected Areas in Communications, vol.28, no.6, pp. 928-935, Aug. 2010.

[4] L. G. Kazovsky, Claus Popp Larsen, Dirk Breuer, Anders Gavler, Mikhail Popov, Kun Wang, Gunnar Jacobsen, Erik Weis, Christoph Lange, Shing Wa Wong, She-Hwa Yen, Vinesh Gudla, and Pegah Afshar, "European and American Research Toward Next-Generation Optical Access Networks," ICTON Conference, Munich, Germany, June 2010. Plenary talk.

[5] L.G. Kazovsky, S.-W. Wong, V. Gudla, P. T. Afshar, S.-H. Yen, S. Yamashita, and Y. Yan, "Challenges in Next Generation Optical Access Networks: Addressing Reach Extension and Security Weaknesses," IET Optoelectronics Journal, special issue on Next Generation Optical Access (invited paper; 2011).

MPLS-TP Update

Monique J. Morrow
Cisco Systems, Switzerland.

Much has been written about MPLS-TP and the purpose of this article is to provide a status of MPLS-TP, stating up front that at the IETF-79 meeting held in Beijing, PRC, November 7-12, that the IETF leadership asserted its support for a single solution, e.g MPLS-TP.

The MPLS Transport Profile (MPLS-TP) is the set of MPLS protocol functions and extensions that support the construction and operation of packet-switched transport networks. In 2008, the IETF and ITU-T entered into an agreement to develop the MPLS-TP standard, which became known as the Joint Working Team on MPLS-TP (JWT) Agreement and is documented in the IETF RFC 5317. According to this Agreement, the development of standards for MPLS-TP is to be carried out within the IETF with requirements input from the ITU-T.

MPLS-TP OAM functions are intended to build on the foundations of existing IP/MPLS technology by providing enhanced capabilities in the areas of connectivity verification, alarm and defect reporting, performance measurement and monitoring, and diagnostic tools. These functions are required to be able to operate both with and without the presence of IP in the network.

The requirements of MPLS-TP OAM have been jointly approved by the ITU-T and the IETF and have been published as RFC 5860, "Requirements for OAM in MPLS-TP Networks". The basis of the requirements, and a keystone of the MPLS-TP OAM protocols, is that they should provide the complete set of OAM capabilities that are both supported by legacy transport network technologies and applicable in packet-switched networks, and that this should be accomplished using protocols that:

- are backward-compatible with existing MPLS protocols
- form a sound basis for the future development of MPLS technology
- are consistent with best practices for Internet protocol design.

There are Internet Drafts within the IETF that are on Standards Track and accepted as MPLS Working Group Drafts that define the OAM toolset for MPLS-TP.
These are:

- ***MPLS Fault Management OAM*** (draft-ietf-mpls-tp-fault)
- ***LSP-Ping and BFD encapsulation over ACH*** **(**draft-ietf-mpls-tp-lsp-ping-bfd-procedures**)**
- ***Proactive Connection Verification, Continuity Check and Remote Defect indication for MPLS-TP*** **(**draft-ietf-mpls-tp-cc-cv-rdi**)**

There are other Individual Drafts, written initially under the guidance of the former MPLS-TP IETF/ITU-T Joint Design Team (aka the MEAD team), which are expected to become Standards Track MPLS Working Group documents.

These are:

- ***Packet Loss and Delay Measurement for the MPLS Transport Profile*** **(**draft-frost-mpls-tp-loss-delay**)**
- ***MPLS On-Demand Connectivity Verification, Route Tracing and Adjacency Verification*** **(**draft-nitinb-mpls-tp-on-demand-cv**)**
- ***Operating MPLS Transport Profile LSP in Loopback Mode*** **(**draft-boutros-mpls-tp-loopback)

In summary:
It is expected that the core OAM documents are expected to be ready between Q4/2010 and Q1/2011,.
For MPLS-TP Interoperability testing conducted by ISOCORE and reported to the IETF at the IETF-79 meeting:
http://www.ietf.org/proceedings/79/slides/mpls-21.pdf

Ethernet Support for Time Synchronization Protocols (IEEE P802.3bf)

Marek Hajduczenia[1,2], *Member IEEE*, Henrique J. A. da Silva[2], *Member IEEE*, Steve Carlson[3], *Member IEEE*, David Law[4], *Member IEEE*

[1] *ZTE Corporation, Network Product Department, Rua Carlos Alberto da Mota Pinto 9, 6a, Amoreiras Plaza, Lisbon, Portugal*
[2] *Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores, Universidade de Coimbra, Pólo II, 3030-290 Coimbra, Portugal*
[3] *High Speed Design, Inc., Portland, Oregon, USA*
[4] *Hewlett-Packard Ltd, Musselburgh, Scotland*
[*] *Corresponding author: marek.hajduczenia@zte.com.cn*

This paper presents an overview of one of the new IEEE 802.3 projects, namely the Ethernet Support for Time Synchronization Protocols, with the working designation of IEEE P802.3bf. This project is chartered with delivering an Ethernet PHY agnostic solution for the support of network synchronization protocols, namely IEEE P802.1AS and IEEE 1588v2, while minimizing changes into the existing Ethernet PHYs and maintaining the layering rules of the Ethernet transport solutions. In this paper we examine briefly the history of IEEE P802.3bf and the adopted architecture, as well as operation of the newly specified Time Synchronization Service Interface (TSSI), providing indication of the transmission and reception of Ethernet frames in the IEEE 802.3 stack. Such information, when combined with the PHY specific ingress and egress latency data, can be used directly to derive the reference plane information required for all synchronization calculations.
Keywords: IEEE P802.3bf, IEEE P802.1AS, IEEE 1588v2, Time-of-Day (ToD), synchronization, TSSI, SFD indication, MAC, MAC Control, MAC Client

Introduction

Synchronization in transport and access networks has become an important topic, especially taking into consideration the incredible growth of packet-based applications in the areas of digital content distribution, video and audio systems with remote streaming, or even mobile backhauling. All these application areas require not only delay-guaranteed, engineered and strictly controlled links (in terms of QoS, bandwidth and jitter), but also the ability to synchronize with a common reference clock to assure proper operation of specific features of the given application. In the case of digital video distribution systems, a critical feature is lip-sync, where the audio and video tracks streamed from a remote content server must be synchronized to avoid unexpected and unintentionally hilarious effects. For the case of audio distribution systems deployed in large buildings, individual speakers have to be synchronized to avoid echo and duplication effects. All mobile access protocols also require some sort of synchronization, to guarantee their proper operation.

Such application requirements, combined with the ubiquitous nature of Ethernet, created a requirement to provide a standardized solution at the IEEE 802.3 layer, capable of supporting synchronization protocols operating on top of 802.3 PHYs. IEEE P802.1AS is an example of such a protocol. IEEE 1588v2 is also well-known, used predominantly in transport systems and in the access domain, especially when connected with the next generation all-IP base-stations (3G and 4G equipment).

Synchronization in Ethernet – background information

Before the IEEE P802.3bf Task Force (TF) was formed, work on Ethernet time synchronization started in 2004 within the Residential Ethernet Study Group (RESG) of the IEEE 802.3 Working Group. Ultimately, the RESG came to the consensus that such a project was better suited for the IEEE 802.1 WG, which deals with management and higher functional layers of the OSI stack.

The IEEE 802.1 WG created the Audio-Video Bridging Group (802.1 AVB), with the understanding that, in the future, the IEEE 802.3 hardware support for the IEEE 802.1 synchronization mechanism would be developed. The IEEE P802.3bf TF formed in January 2010, after the formation of the Time Sync Study Group in July of 2009, is the project that is chartered with writing an amendment to the IEEE 802.3 base standard. Informal discussions took place for almost two years between members of the IEEE 802.1 AVB group and members of IEEE 802.3 to hone in on the functional requirements for the target project.

Other possible solutions exist for implementation of synchronization over Ethernet, such as IEEE 1588v2, which has had to operate for years without a standardized hardware support, as well as Synchronous Ethernet (SyncE), specified under ITU-T Recommendation G.8262 (see http://www.itu.int/rec/T-REC-G.8262). While IEEE 1588v2, being part of the service layer solutions for synchronization, can benefit from IEEE P802.3bf, SyncE cannot,

requiring specific non-IEEE 802.3 standard changes in individual Ethernet PHYs to guarantee clock synchronization between ingress and egress ports.

IEEE P802.3bf *TimeSync* Task Force

Objectives

The objectives of the IEEE P802.3bf *TimeSync* Task Force can be divided into the official one, as recorded in the Project Authorization Request (PAR), and the" unofficial" ones that most IEEE 802.3 projects strive to meet.

The primary goal of this project (and its official objective) is to "provide an accurate indication of the transmission and reception initiation times of certain packets, as required to support IEEE P802.1AS". In the course of discussions with IEEE P802.1AS, it was established that:

(1) higher 802.1 layers will have the ability to correlate the transmitted P802.1AS frames and indications received on the Time Synchronization Service Interface (TSSI);
(2) in order to maintain complete transparency of the method adopted by P802.3bf, each frame passing through the Medium Independent Interface (xMII), irrelevant of the data rate of the underlying PHY, will generate an indication on the TSSI; and
(3) higher layers (TSSI client) will require access to information on the ingress and egress delay through the PHY.

In addition, several objectives were self-imposed by the *TimeSync* Task Force, namely:

(1) limiting changes to the IEEE 802.3 base document, especially existing clauses;
(2) providing a PHY agnostic solution, capable of supporting both existing and future IEEE 802.3 PHYs; and
(3) delivering an open architecture, guaranteeing scalability together with the progress of future IEEE 802.3 projects.

Architecture

The IEEE P802.3bf architecture is presented in Figure 0-1, in the framework of the existing IEEE 802.3/802.1 layers. This project introduced three major new features into the existing IEEE 802.3 stack, namely:

- Rx SFD Detect and Tx SFD Detect functions, located in the RS sublayer, responsible for detecting the transition of the SFD (Start of Frame Delimiter) associated with the reception and transmission of an Ethernet frame, respectively. It must be noted here that SFD indications are generated for all Ethernet frames, regardless of whether these are client frames or MAC Control frames, as explained in more detail in sections 0 and 3.4, for the transmit and receive directions, respectively.
- TSSI (Time Sync Service Interface), associated with two new indication primitives, i.e. TS_RX.indication generated by the Rx SFD Detect function and TS_TX.indication generated by the Tx SFD Detect function. The TSSI bypasses the existing PLS service interface (PLS SI) between RS and MAC as well as MAC service interface (MAC SI) between MAC and MAC Client, providing direct access to the new RS functions for a Time Sync Client (outside the scope of IEEE 802.3 specifications). A similar approach was also used within IEEE P802.3az to provide signaling in and out of the RS sublayer.
- Managed objects in Clause 30 as well as MDIO registers, providing the Time Sync Client the ability to read ingress and egress latency information, characteristic for the given PHY. This provides the Time Sync Client with the ability to perform necessary synchronization calculations relative to the reference plane located at the bottom of the 802.3 stack (at the MDI).

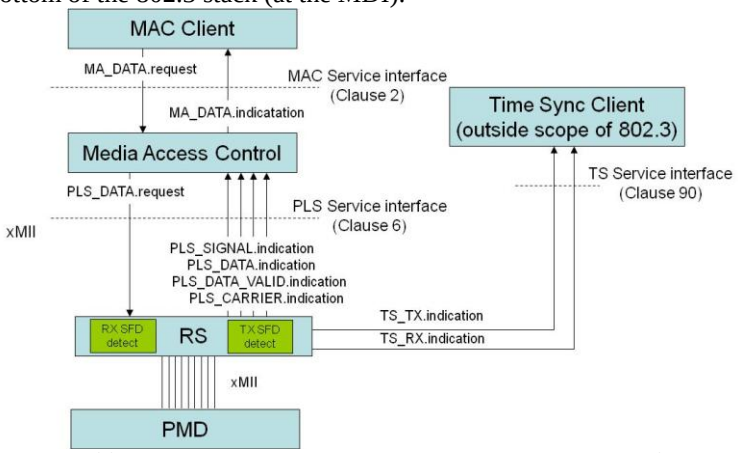

Figure 0-1: Relationship between 802.3bf functions, TSSI and remaining 802.3/802.1 layers. All Clause references relative to IEEE Std 802.3.

Other technical approaches for delivering timing information to the Time Sync Client have been examined during the Study Group phase of the project, including insertion and manipulation of time stamp information fields into the passing synchronization frames. However, given the resulting architectural complications, as well as concerns about layering violation due to operations performed so low in the Ethernet transport stack, such solutions were abandoned in favor of a more generic and layering-friendly approach.

Relationship between primitives in the transmit direction

Figure 0-2 presents a simplified (all temporal relationships are disregarded for simplicity of the drawing) look at various primitives generated at different IEEE 802.3 interfaces, including the newly specified IEEE P802.3bf TSSI (here shown as TS_TX.indication). A single MA_DATA.request is generated by the MAC Client across the MAC SI requesting transmission of a whole frame at a time. MAC is responsible for generating a series of PLS_DATA.request primitives across the PLS SI, sending individual bits towards the PL. Finally, the TX SFD Detect function in the RS sublayer detects the transmission of the first octet of each passing frame (SFD), generating the TS_TX.indication primitive towards the Time Sync Client, whenever an SFD is detected.

The figure in question also demonstrates the need for correlation between frames sent by the MAC Client (Time Sync Client in this case) and the TS_TX.indication primitives received on the TSSI interface. In the case of two first frames (marked as green), they can be considered as generated by the Time Sync Client and the associated TS_TX.indication primitives can be easily correlated with the transmitted frames. The third frame, marked as red, is generated locally by the MAC Control Client (e.g. MPCPDU). In this case, the Time Sync Client is not aware of such a frame and will only receive the associated TS_TX.indication primitive, which it will not be able to correlate with any data transmission and should therefore be discarded.

The functions and behavior of the Time Sync Client are not specified within IEEE P802.3bf, and thus the description presented above is based on logical expectations of its performance.

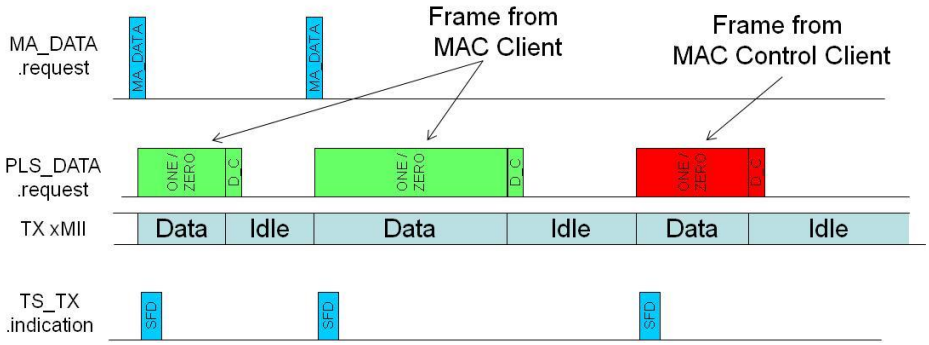

Figure 0-2: Relationship between primitives at various IEEE 802.3 interfaces (simplification).

Relationship between primitives in the receive direction

Likewise, Figure 0-3 presents the same type of simplified relationships between primitives generated at different IEEE 802.3 interfaces, including the newly specified IEEE 802.3bf TSSI (here shown as TS_RX.indication).

The Rx SFD Detect function located in the RS sublayer continuously scans the receive data stream, and generates a TS_RX.indication primitive whenever a correctly formed SFD is detected in the passing data. Existing IEEE 802.3 primitives are responsible for the transfer of data between the RS and MAC (using a series of PLS_DATA.indication primitives) and next between the MAC and MAC Client (here assumed to be the Time Sync Client) using a single MA_DATA.indication primitive per frame.

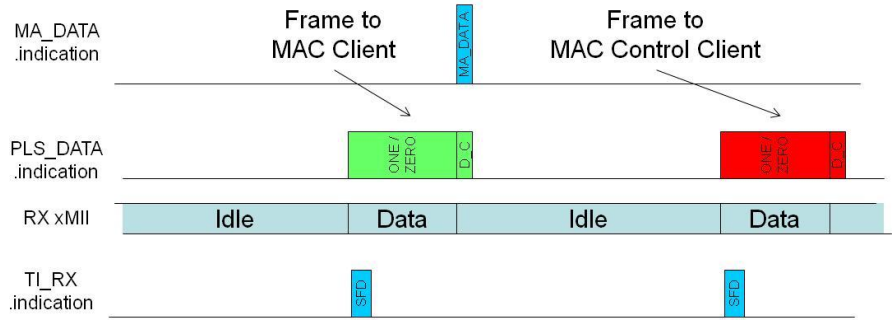

Figure 0-3: Relationship between primitives at various IEEE 802.3 interfaces (simplification).

Similar to the transmit case , in the receive direction it is also possible for Ethernet frames to be addressed to the MAC Control Client (marked in red in Figure 0-3), in which case the Time Sync Client is expected to ignore the associated TS_RX.indication primitive, given that there is no received frame at the MAC Client level.

Applications of IEEE P802.3bf TSSI

IEEE P802.3bf was originally designed to provide direct support for the IEEE P802.1AS Time Sync Client, operating on top of IEEE 802.3 PHYs. Long-term cooperation between both groups, as well as technical communications between experts, resulted in a specific architecture, which is both data rate independent and PHY agnostic. This means that it can be applied to any existing or future Ethernet PHYs, with its applicability limited only by the data flow sink capabilities of the Time Sync Client.

In the course of architectural work in IEEE P802.3bf, it was quickly understood that potential applications of the newly specified TSSI could also cover other synchronization protocols, e.g. IEEE 1588v2 and other proprietary use cases, which can benefit from information about transmit and receive path latencies as well as identification of the frame transition event through the RS sublayer. The potential use of IEEE P802.3bf to support IEEE 1588v2 resolves one of the long-standing problems of this specific synchronization protocol, namely the lack of a standardized way to retrieve correlated information between the frame transmission time and synchronized time. Various proprietary mechanisms have been developed over the course of the last few years, some of them quite similar to the solution proposed in IEEE P802.3bf. It is expected that the TSSI will become a de-facto standard for the future implementations of IEEE 1588v2 protocol operating on top of Ethernet PHYs.

Summary

IEEE P802.3bf provides one of the critical pieces in the overall puzzle of synchronization over packet networks. The pervasive nature of Ethernet technology, covering various flavors of copper, optical, and wireless IEEE 802 compliant media, providing transmission speeds anywhere between 10 Mbit/s and 100 Gbit/s, will benefit substantially from native support for network synchronization protocols such as IEEE P802.1AS and IEEE 1588v2. The selected solution provides a simple event indication via the TSSI to the Time Sync MAC Client, informing it about the transmission or reception of an Ethernet frame, relying on the capability of the said client to perform correlation between sent/received data and primitives. The open and scalable nature of the specified solution, as well as its very simple character, fit very well into the specific nature of Ethernet networks. It is expected that, within the next few years, support for IEEE P802.3bf becomes wide spread for all new Ethernet PHYs, especially the ones intended to be used in applications requiring hardware support for synchronization and time-stamping for the passing frames. This project also marks another successful, long-term cooperation between the IEEE 802.1 and IEEE 802.3 Working Groups, indicative of the tightening relationship between the management and physical layers in Ethernet.

More information about the project

Primary website
http://www.ieee802.org/3/bf/
Public folder
http://www.ieee802.org/3/bf/public/index.html
Private folder (including the draft)
http://www.ieee802.org/3/bf/private/
IEEE 802.3bf PAR
http://www.ieee802.org/3/bf/P802.3bf.pdf
IEEE 802.3bf 5 Criteria
http://www.ieee802.org/3/time_adhoc/P802_3bf_5Criteria_802_3_approved_1109.pdf
IEEE 802.3bf Objectives
http://www.ieee802.org/3/time_adhoc/P802_3bf_objective_802_3_approved_1109.pdf
E-mail reflector
http://www.ieee802.org/3/bf/reflector.html

Ethernet Service Protection Over External Interfaces

Zehavit Alon, Nokia Siemens Networks, Israel

Abstract: Over the last few years, packet switching technologies, such as Ethernet and MPLS, have been widely adopted by the industry as the technologies of choice to replace existing networks based on circuit-switching technologies, such as SONET/SDH and ATM.

Circuit-switched network technologies provide mechanisms that guarantee sub-50ms service protection for their customers. The same protection level must be provided by the different packet technologies in order to retain the identical set of capabilities formerly granted to the customer, so that packet technologies can seamlessly replace circuit technologies.

The various packet technologies define different ways of protecting a service within the network. However, all the currently defined protection methods are intra-network only and there is no standard method for protecting services against node failures at the edges, i.e. over the external interfaces, i.e. for protecting connectivity between attached networks.

Figure 4 illustrates a theoretical packet based network where one of the services that spans several service providers is emphasized.

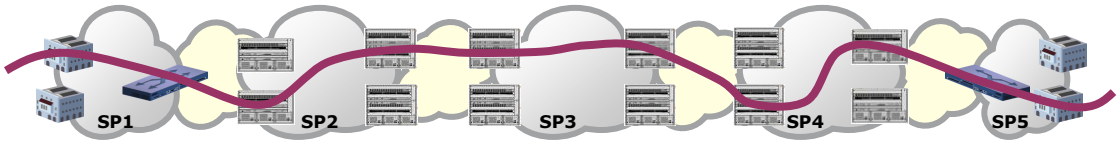

Figure 4: Example of a service spanning several service provider networks

The goal of this paper is to introduce a mechanism aiming at providing a robust solution for the missing capability. This paper describes the following: (i) Overview of the current state, (ii) required functionality that does not exist as yet and (iii) a proposed mechanism for protection between domains, the Inter Network Service Protection (INSP)

Abbreviations

- ENNI - External Network to Network Interface
- INSP - Inter Network Service Protection
- IZ – Interconnection Zone
- LAG – Link Aggregation
- SG - Service Gateway
- UNI - User to Network interface
- VLAN – Virtual LAN

Definitions

This section describes the definitions used throughout this paper (Some definitions are accompanied by a figure to clarify the definition).

- ***Border Node*** – A node that that resides at the edge of the network and connects it to another network. MEF external interfaces are located on border nodes.

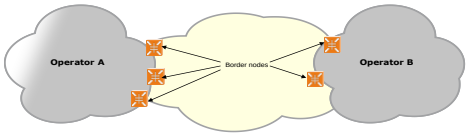

Figure 5: Border Nodes

- ***Domain*** - A portion of a network. A collection of network elements within a common realm of address space which are operated as separate administrative domains.

- ***ENNI*** – ENNI is a reference point representing the boundary between two operator networks that are managed as separate administrative domains.
- ***External Interfaces (EI)*** – Interfaces between domains, including ENNIs and UNIs
- ***External Link –*** A link connecting the border nodes of attached domains. Can be physical or logical (i.e. LAG)

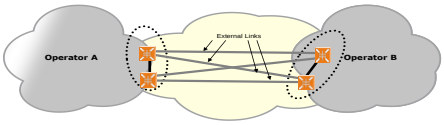

Figure 6: External Links

- ***Interconnection Zone (IZ)*** – A realm that includes the border nodes of two connected domains and all the links connecting these border nodes (internal and external) that participate in the service protection mechanism

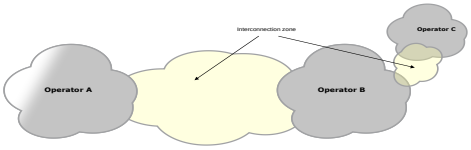

Figure 7: Interconnection Zone

- ***Internal Link*** – A link that connects two border nodes within the same service portal. Can be physical or logical i.e. can be a LAG

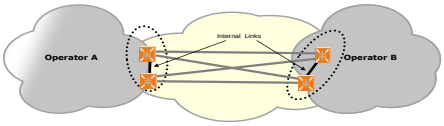

Figure 8: Internal Links

- ***Inter Network Service Protection (INSP) –*** A mechanism for providing service protection over external interfaces
- ***Network*** – A number of domains connected to each other
- ***Service*** – An Ethernet service that is designated by a VLAN. The VLAN can be C-VLAN, S-VLAN or B-VLAN and for the sake of simplicity, this term is used throughout this document to represent both a single VLAN and a group of VLANs that are handled together and not as individual VLANs. A group of VLANs are sometimes referred to as a "service bundle".
- ***Service Portal*** – A logical entity that groups all the border nodes inside a domain which protects a specific service. A service portal in one domain is connected to exactly one other service portal in another domain. ***Portal*** – A is a logical entity that gathers all the service portals of a domain facing the same IZ, i.e. a portal includes all the border nodes facing the same IZ.

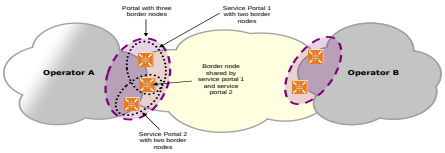

Figure 9: Service portal and Portal

- ***UNI –*** Physical interface/demarcation point between the service provider and the customer. It also represents the service start/end points.

Introduction

As the communication infrastructure nowadays has a global reach, a service may extend across a network built of several domains, each of which may employ a different technology and a different protection mechanism.

Domains are connected by external interfaces. The MEF has defined two major types of external interfaces – User to Network Interface (UNI) and External Network to Network Interface (ENNI). Service packets transit both UNI and ENNI interfaces. To enable end-to-end service protection capable of protecting against multiple failures, each

domain should protect the service locally. In addition, the service should be protected in the area between the domains, that is, in the interconnection zone where the networks are connected.

While different local protection mechanisms exist and provide protection within domains, no similar standard mechanism for node protection exists .

It is desirable that any protection mechanism for the interconnection zone complies with all Ethernet characteristics and QoS parameters and in addition limits the effects of component failure or performance degradation with the result that remote parts of networks remain unaffected by these events.

Protection mechanism

A protection mechanism for the IZ should operate on nodes in the border of each domain and on links connecting these border nodes in different connectivity structures. It should employ a mechanism for failure detection and a mechanism to overcome these failures.

Failure detection

Failures in connectivity and degradations in service performance can be detected by physical means and by OAM methods defined by IEEE 802.1ag and Y.1731.

Interconnection Zone structure

The composition of the IZ, i.e. the number of border nodes, internal links, and external links, and the way border nodes are connected to each other inside the service portal and between service portals of attached domains may vary in different domain configurations.

The border nodes protecting a specific service in the domain, facing a specific attached domain, are grouped in a logical entity called the service portal. (One or more service portals can be contained within one interconnection zone and a border node can be shared by a number of service portals). The number of nodes in each service portal greatly influences the level of protection and the quality that a service is granted. A service portal containing a single node can provide only link protection and can not protect against node failure. A service portal containing two border nodes can provide better protection, as it can provide both node and link protection. Additional nodes may be added to a service portal. However, the author of this document is of the opinion that this is unnecessary, since two border nodes can provide the required functionality.

Theoretically, any topology can be used for the IZ. In some cases, one topology may be more advantageous than others. The topology of choice for an operator varies according to the services provided, the network span, the connectivity between domains and the distance between significant elements in the network. The following topologies may be considered: ring, hourglass and full mesh.

In ring topology each border node is connected to no more than two other border nodes; one node must reside in the same service portal while the other node must be located in the attached service portal.

Hourglass topology comprises border nodes connected by external links only. In an hourglass topology, each border node of a service portal in one domain is connected to all border nodes of the service portal in the attached domain. In this topology, every instance of component followed by protection switching is propagated to the attached domain.

In a full-mesh topology, each border node is connected to all other border nodes in the IZ. Every border node in one service portal is connected to all border nodes in the attached service portal by external links, and within the service portal, all border nodes are fully connected by internal links. This topology is capable of isolating a link failure ensuring that it is handled within the IZ and is not propagated outside the IZ**.** Figure 10 depicts four nodes ring, hourglass and full-mesh connectivity.

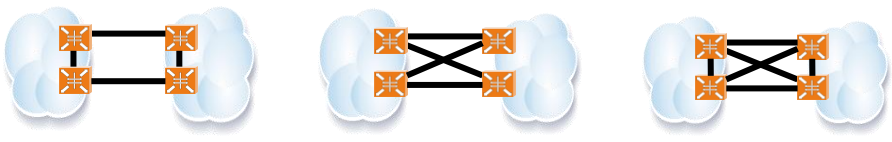

Figure 10: Ring, hourglass and full-mesh connectivity

Inter Network Service Protection mechanism

One possible way in which the required protection capabilities can be provided to UNIs and ENNIs is to use the proposed Inter Network Service protection (INSP) mechanism (explained below). The proposed mechanism ensures that service traffic will always have a path through the IZ and will be able to reach the attached domain while complying with the Ethernet characteristics and QoS parameters. The INSP supports all the constructs mentioned previously and isolates failures and protection switching events when the topologies where this is feasible.

INSP principle of operations

In the INSP mechanism, each domain allocates a service portal to each service that should be safely delivered between connected domains. When a service portal includes more than one border node, node protection can be achieved in addition to link protection.

At any point in time, only one of the border nodes in a service portal is allowed to convey traffic from the domain to the IZ and from the IZ to the domain. This border node is called the *service gateway (SG)*. The SG is dynamically elected by the service portal according to the status of the domain and the IZ to which it belongs. Since the domain is dynamic, the SG may change when entities inside the IZ fail and recover. As the service portal holds only one SG (the border node that handles the service packets) at any given moment, it is guaranteed that service packets enter once only from the domain to the IZ, and once only from the IZ to the domain. Packets that are received by border nodes other than the SG are dropped, regardless of whether they were received from the IZ or from the domain. Assigning one of the border nodes in each service portal to be the service gateway guarantees that a packet will not be duplicated.

Figure 11 depicts an example of a service and its SGs in Operator A and in Operator B.

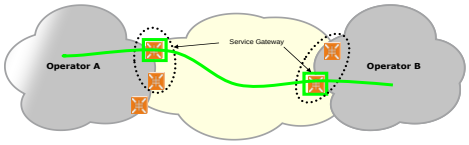

Figure 11: Service Gateway

It is desirable that the service traffic is co-routed inside the IZ (to enable learning). This is achieved by choosing one of the two domains SGs to select the link over which traffic is conveyed to the attached domain. This SG is referred as the initiating SG. (If both SGs were to select the link, the path could diverge and transmitted and received traffic would not use the same path in the IZ). The second domain expects to receive service packets over the link selected by the first domain and does not select a link for that service.

If the selected link directly connects the SGs of both domains, traffic received by the SG from the IZ is forwarded by the SG directly to the domain.

Figure 12 shows an example of two attached domains where the SG in one domain is connected directly to the SG of the other domain.

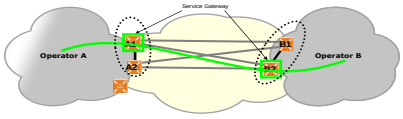

Figure 12: Directly connected SGs

If the selected link is connected to a border node that is not an SG, this border node redirects received traffic to the SG in its service portal, and the SG transmits it to the domain.

Figure 13 depict examples of attached domains where the SG in one domain is not directly connected to the SG of the other domain. These examples show the SG connected through an intermediate border node via an internal link to the SG of the attached domain.

Figure 13: SGs not directly connected in full-mesh and ring topologies

As the INSP operates per service, it is possible to define specific border nodes as the initiating SGs (select the active link) for some services, and as the SGs that accept the selected link for other services. Load sharing can be achieved by defining the different border nodes as SGs for different services.

The health of the IZ components is monitored by OAM messages sent frequently enough to comply with the protection time restriction. When a failure or degradation is detected, the protection mechanism is responsible for selecting an alternate link for the affected services. If the initiating SG fails, a new SG is elected by the service portal and the new elected initiating SG selects a link and if a link failed an alternate link is selected.

As Ethernet aims to prevent frame mis-ordering as much as possible, the SG (which is the only border node that handles a service) ensures that only one port is allowed to send and receive service packets at any given moment. The order of operation when selecting the link over which the service will be conveyed is as follows: first disable the active port and only then enable the new port. With this paradigm of "break-before-make", packet ordering is preserved as packets are handled from one queue at a time.

One of the requirements for an external interface protection mechanism is that it should minimize the effects of a failure in the IZ on the attached domains. This requirement can be fulfilled for link failures when the IZ contains internal links that can be used to bypass a failed link without changing the SG, and as the SG is not changed, the attached domain is not affected.

Figure 14 depicts a scenario where the topology is full mesh. When the active external link fails, a new link becomes active. As the alternate, external link is connected to a non SG border node this node seamlessly relays the traffic over an internal link connecting it with the SG in its service portal. Although the path before and after the failure differs, the SGs in both domains were preserved and were not changed. This functionality is beneficial as it isolates the link failure in the IZ in a way that prevents the propagation of failure effects outside the IZ. On the other hand, this functionality is only supported when internal links exist between border nodes in the service portal and can relay received traffic to the SG.

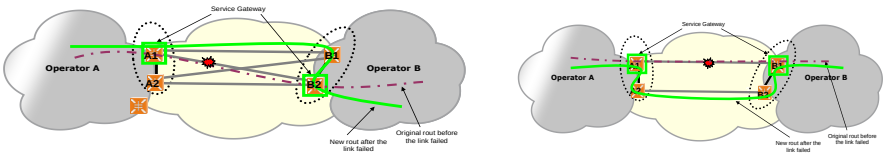

Figure 14: Bypass of external link failure in full mesh and ring topologies

When possible, a bypass inside the service portal is created. The attached service domain plays no part in this functionality. Each domain determines by itself, whether and when to use the internal links for bypass functionality.

The initiating SG selects the link that will be used for the services it supports. The preferred link is one of the external links which directly connects the two SGs of the attached domains. If no such external link is available, another external link is selected and if such a link is not available either, an internal link is selected. Traffic will eventually reach the SG assuming that the border node that receives the service traffic will be able to transfer it to the SG.

The INSP mechanism follows all the Ethernet functionality as defined by 802.1Q and its amendments. It does not modify the frames size in order to perform the protection switching, and its queuing functionality is also not modified so it continue to handle priority as defined by 802.1Q.

INSP advantages

1. Provides a full solution for protection of external interfaces and does not rely on non standard functionality
2. Stand alone mechanism, as intra-domain protocols, mechanisms and configurations should not be modified to support the proper functionality. All protocols inside the attached domains do not require modifications.
3. Minimize packet duplication
4. Minimize packet disordering
5. Guarantees the prevention of fault propagation beyond the IZ in all topologies that support this functionality
6. Scalable, as all the protected services are monitored by one message and the protection state is coordinated by one message for all aggregated services.
7. All services can be supported by one dedicated, internal link without encapsulation. When the internal link is shared by the IZ and the domain, i.e. the domain uses this link for relaying traffic inside the domain,

traffic belonging to the IZ need to be distinguished from the intra-domain traffic. All the IZ traffic can be tunneled in one tunnel and do not have to have a dedicated tunnel per service. on the internal link there is no need for a dedicated, internal link (physical or logical) for each and every service.

8. One protocol is used on all links – external and internal and the intention is to make it standard. As the same (standard) protocol is used inside and outside the portal, the mechanism allows interoperability, since it is capable of operating in a mixed environment both inside the portal and between portals - does not assume that a single vendor will be used.
9. Supports topologies such as mesh (full and partial) and ring
10. Supports physical ports as well as LAG, so that service BW can be increased as the service grows
11. Provides simple network expansion through the addition of a domain as service protection using INSP only requires the configuration of border nodes
12. Provides simple indication on the protection state

Current standardization status

The IEEE802.1 working group has been discussing this issue since the middle of 2009. It is highly probable that a new project dealing with external interface protection will be initiated in the first half of 2011.

The MEF is working on defining requirements for protecting external interfaces; this project is currently in the ballot phase.

Summary

It is evident to the industry that a protection mechanism is required in the IZ. The IEEE is currently discussing possible solutions that will provide a standard mechanism. Such a mechanism will make networks more robust and ensure that the degree of availability defined in the agreement is maintained. A standard protection mechanism will enable service providers to purchase equipment from several vendors and install it in the network boundaries; providers will therefore be better placed to negotiate with the vendors. In the event of equipment failure, the mechanism will prevent the malfunction from occurring in both border nodes. In addition, it will enable gradual upgrades and replacements to be performed, as well as the standard management of installed equipment. The INSP is a mechanism that can fulfill all those requirements.

References

1. IEEE Std 802.1Q, 2008 Edition, Virtual Bridged Local Area Networks
2. MEF 20 (UNI); MEF 26 (ENNI)

About PRISM (***www.ontc-prism.org***)

***Aim*:** To disseminate relevant content pertaining to optical networking and related growth areas across industry and academia. To promote the growth of optical networking activity by creation of a unified knowledge base. To create a communication bridge between industry and academia in terms of research frontiers and complementary strategies for future growth.

***Scope*:** The optical networking community stands at a point where its potential is not fully realized. The bandwidth offered by the fiber at price points that currently prevail is a fantastic business case for Internet services for providers the world over. Optical networking has transcended itself from a point-to-point communication service to a WDM based multi-point granular networking hierarchy. This journey was made possible through successful and important innovations in the optics and networking domain, bringing together a rich technology set for deployment in telecommunication networks. It would be fair to say that without optical networking, the scope of the Internet would not reach its global scale that it has presently reached. In the future, optical networking has the potential to impact the telecom world through new innovations in architecture, protocol and devices that would lead to new service offerings impacting human lives. Amongst these futuristic offerings are cloud computing, energy efficient systems, data-centers, 100 Gigabit Ethernet, WDM PON, multi-point communication systems, sub-wavelength grooming and transparent ROADM-based services. It is clear, and especially pronounced in Asia and parts of Europe that optical networking will play a very important role in the design of future networks. Whether it is the GENI project in the US or the Akari in Japan – optical networking finds a clear way into technological offerings for the future of the telecommunication industry. From a historical perspective, optical networking has offered significantly to the telecom industry – we distinctly note that after the telecommunication bubble burst, it was the area of metropolitan networks that led to the re-bounce of telecommunications the world over. It is always important to highlight such historical perspectives from industry leaders and pioneers to bring the optical community closer. We continue to exploit the latest advances in this area of telecommunications – delving on the research and development of optical networking solutions.

The scope of the newsletter is as follows:

- A forum that brings the optical networking community together, through leadership articles in technology and research.
- Bring to the fore issues that both industry and academia are working on, with the focus of being able to minimize this gap through interaction via the newsletter forum.
- Highlight important events related to the area of optical networking, in particular focus on consortiums, projects, awards, seminal breakthroughs, standards and industry related information.
- Research: Focus on research issues pertaining to optical networking. Showcase key growth areas (like data centers, metro ROADMs, 100GE, etc.).
- Consortiums and Projects: Focus on consortiums and projects relevant to optical networking, in which the primary entities are research focused (non-profit groups like universities etc.)
- Developing Economies: Focus on emerging economies and the networks there.
- Standardization activity: The newsletter will periodically discuss standard related activities especially when new drafts are circulated or a standard in form of an MSA is accepted. A standard pioneer will be invited to write about the standard. Our focus will be on the IEEE 802 working group, the ITU groups and FSAN groups in terms of coverage.
- Industry information: latest *technical* happenings will be reported from the industry. These will be critically based on demonstrations at international tradeshows such as OFC, ECOC and World Broadband Forum. Care will be taken not to report any company specific information and ensure vendor neutrality in the newsletter.
- Service provider focus: Since a key consumption point of our industry are service providers, it is most important to focus a section of the newsletter on them. We will in every newsletter focus on the latest happenings in the provider space – whether it is adoption of new technologies or new deployments or even network designs, we will cover these through neutral writings. In particular, we will ensure that no names are taken in the coverage, making it generic – for example, "a select provider in the North America has decided to deploy ROADM technology using WSS cross-connects [source]..".
- Periodically create a roadmap of technologies in different domains pertaining to optical networking. The roadmap would be a team effort by multiple experts in association with the editor.
- Optical Networking is Fun (ONiF): a section devoted to humor in optical networking – puzzles, crosswords and "did you know" for after-hours research.

Submit your article as a .pdf file to submissions@ontc-prism.org. Note that you must have a covering note that descibes the nature of the article from one of the above scope keywords. **The scope keywords are: consortiums, projects, growth areas, emerging economies, Standardization activity, Industry information, Service provider focus, roadmap of technologies and Optical Networking is Fun.**

Note to prospective authors: ONTC Prism follows strict policies mandated by the IEEE Code of Ethics. We will strongly enforce plagiarism and self-plagiarism as a review criteria. For more information visit:http://www.ieee.org/web/publications/rights/ID_Plagiarism.html.

Ashwin Gumaste,
James R. Isaac Chair,
Department of Computer Science and Engineering
Indian Institute of Technology Bombay,
Contact Information:
Room 208, Kanwal Rekhi Building, IIT Bombay, Powai, Mumbai, 400076
Email: ashwing@ieee.org, Web: www.ashwin.name.