Providing Resilience for Carrier Ethernet Multicast Traffic

SARAH RUEPP, HENRIK WESSING, JIANG ZHANG, ANNA V. MANOLOVA,
ANDERS RASMUSSEN, LARS DITTMANN, MICHAEL BERGER
DTU Fotonik
Technical University of Denmark
Oersteds plads, building 343, 2800 Kgs. Lyngby
Denmark
srru@fotonik.dtu.dk

Abstract: This paper presents an overview of the Carrier Ethernet technology with specific focus on resilience. In particular, we detail how multicast traffic, which is essential for e.g. IPTV can be protected. We present Carrier Ethernet resilience methods for linear and ring networks and show by simulation that the availability of a multicast connection can be significantly increased by applying relevant resilience techniques.

Key–Words: Carrier Ethernet, Resilience, IPTV, Simulation

1 Introduction

The path towards profitable operation of networks is paved with emerging premium services with strict requirements to bandwidth, delay, packet loss and resilience. Examples are IPTV, Video on Demand (VoD), Videoconferencing and telemedicine. They all uses IP on the packet layer but they demand reliable underlying transport networks for proper quality of experience (QoE). In a telemedicine video streaming application, where a doctor with special expertise remotely acts as second opinion, resilience is obviously required. In addition, such a service has strict delay bounds, which demands fast recovery and good picture quality (i.e. QoE). Other services like IPTV require multicast transport, and the ability to quickly identify and isolate a faulty situation in a complex multicast architecture can make the difference between profitable or non-profitable operation. The demand for high quality reliable services further increases the complexity, when the range of the services extends the local network, and multi-domain issues arise. Hence, a standardized connection monitoring is required to proactively avoid most errors and to swiftly react to the remaining. Carrier Ethernet technologies address these challenges by adding transport functionalities including resilience to an MPLS-like network architecture.

To use Ethernet as a transport technology for large-scale deployment, features such as network layer architecture, customer separation and manageability must be added. By using PBB-TE [8] and T-MPLS [9], Ethernet can be used as a transport technology. Triple Play services, in particular IPTV, will be the main driver for Carrier Ethernet. But a number of challenges must still be solved. This includes enhanced Operations and Management (OAM) functions as well as survivability. T-MPLS defines its protection capability using ITU-T's Recommendations G.8131 [2] (T-MPLS linear protection switching with 1+1, 1:1 and 1:N versions) and G.8132 [3] (T-MPLS ring protection switching).

This paper addresses how Carrier Ethernet technologies can be used in the transport network to provide resilience to the packet layer. In section 2 we present the Carrier Ethernet techology including an analysis of the relevant requirements and standards. In section 3 we outline the different failures that can occur in Carrier Ethernet networks and which challenges the different failure types (both hard and soft) pose on successful recovery. Explicit focus is on the multicast situation. Section 4 presents our simulation study and the results. Section 5 concludes the paper.

2 Carrier Ethernet

Carrier Ethernet is based on the existing Ethernet technology. It is however enhanced with specific functions to be applied in metro networks. According to the definition proposed by the Metro Ethernet Forum (MEF), Carrier Ethernet is a ubiquitous, standardized, carrier-class service, which shall be delivered over native Ethernet-based Metro and Access networks and can also be supported by other transport technologies [4]. To overcome the limitation of native Ethernet, Carrier Ethernet adds carrier-class features, such as QoS and OAM, to overcome the limitations of native Ethernet. The MEF defines five specific attributes for Carrier

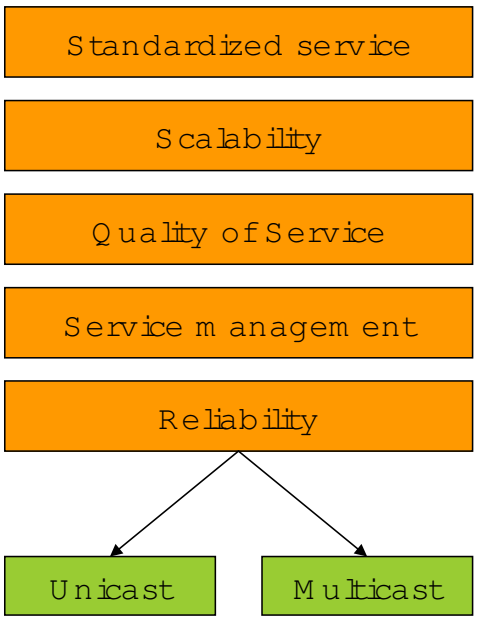

Figure 1: Metro Ethernet Forum requirements towards Carrier Ethernet.

Ethernet to distinguish it from traditional LAN based Ethernet. These attributes include standardized services, scalability, service management, quality of service and reliability. The functions are illustrated in figure 1, and they are the main challenges to be solved in order to establish future transport networks. In the reliability category it is very important to distinguish between reliability for unicast and multicast protection, since multicast protection poses many additional challenges in terms of management and operation.

Standardized service Carrier Ethernet is a ubiquitous service offering global and local services. The E-Line service is used for private line services, Internet access and point-to-point VPNs, while the E-LAN service is applied for multipoint virtual private networks and transparent LAN service. Carrier Ethernet does not require any changes to its equipment or networks while the service is being offered [4].

Scalability Native Ethernet has limitations on scalability, which include the number of discrete users, MAC addresses, service connections, bandwidth options and L2VPN applications [5]. Carrier Ethernet is improved to achieve service scalability to support a multi-customer environment. The use of MPLS provides a suitable control plane that overcomes the shortcomings of native Ethernet control [4].

Quality of Service (QoS) To guarantee a certain level of service, Service Level Agreements that deliver end-to-end performance to meet the requirements of various services should be possible in a carrier network. Carrier Ethernet does not only guarantee end-to-end bandwidth, but also enables service providers to establish connection-oriented SLAs for each classified traffic flow, thus overcoming QoS limitations [6].

Service management When expanding the network from LANs to metro networks that service thousands of subscribers, the ability to monitor, diagnose and centrally manage the network is necessary. Thus carrier-class OAM has been a hot topic within IEEE, MEF and ITU. The standard-based OAM mechanisms can provide SLA measurements, continuity checks and alarm functions.

Reliability To achieve reliability is an important performance factor for communication networks. Carrier Ethernet is not an exception, so it should possess the ability to detect and recover from a variety of network failures within a reasonable timeframe to avoid causing annoyance to the users. The protection mechanisms of native Ethernet are however not suitable for Carrier Ethernet resilience due to speed constraints, and also because emerging multicast services require a plethora of detection, re-routing and management functions to deliver suitable performance.

3 Carrier Ethernet Resilience

Carrier Ethernet networks can be affected by many kinds of failures. In particular, if the Carrier Ethernet network is used for multicasting IPTV traffic, many challenges in the field of network survivability arise. The failures types, as illustrated in figure 2 can be categorized in three different categories:

- Hard failures. The term hard failures covers all the failures where equipment is physically affected by failures. This category covers the well-known problem of cable cuts. Furthermore, it also covers failures where node equipment is affected by physical faults (e.g. power outages, earthquakes, flooding, etc.). This can be either the entire node being out of operation, or only parts of a node (i.e. a few line-cards) being affected.

- Soft failures. The category of soft failures deals with all sorts of software errors. This can be both actual software bugs in the node managment system, as well as failures in the routing protocol. In a multicasting environment, the actual OAM messages can be corrupted. Furthermore, problems with the multicasting tree may arise, which leads to misconfiguration of the distribution tree.

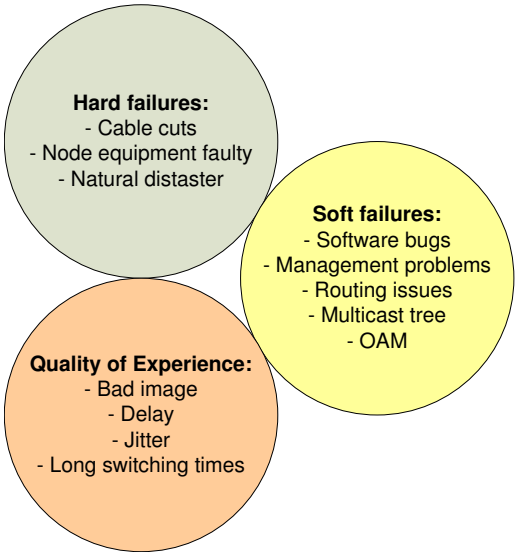

Figure 2: Failure types.

- Quality of Experience (QoE) failures. Failures related to QoE deal with how the users perceive a given failure event. When a user watches IPTV, he or she basically does not care whether there are some faulty situations in the network, as long as they are invisible. But when QoE degrades, the users start complaining, which is bad for the business case. Typical failures in this category relate to bad images (due to physical properties: jitter, delay) and long channel switching times.

When designing resilience concepts for Carrier Ethernet, it is natural to consider whether some existing mechanisms from other communication standards could be reused, for example from Ethernet or MPLS technologies. The following survivability concepts could be considered:

- Ethernet uses the (Rapid) Spanning Tree protocol. However, this is too slow to be suitable for Carrier Ethernet.
- MPLS uses Fast Reroute for recovery. However, T-MPLS does not allow label merging, making the approach impossible.
- MPLS uses global path protection. There is no conflict with T-MPLS and hence the method can be used as a starting point for Carrier Ethernet Resilience.

Figure 3 shows the standardization initiatives for T-MPLS with focus on resilience. T-MPLS defines its protection capability using ITU-T's Recommendations G.8131 (T-MPLS linear protection switching with 1+1, 1:1 and 1:N options) and G.8132 (T-MPLS ring protection switching) Further relevant

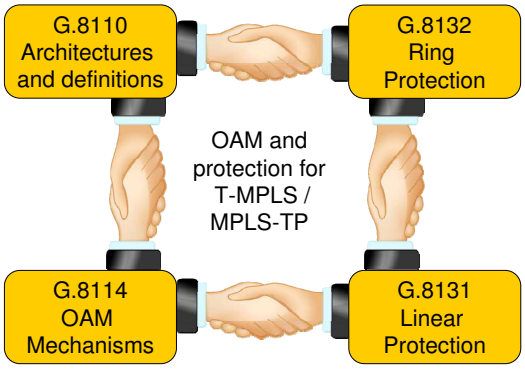

Figure 3: OAM and protection for T-MPLS/MPLS-TP.

standards are G.8110 (Architectures and definitions) and G.8114 (Operation and maintenance mechanism for T-MPLS layer networks).

3.1 Failure detection in Carrier Ethernet

The OAM protocol is used to detect failures of the primary or backup LSPs. According to [1], Connection Verification packets are used to probe the continuity of the connection. They are inserted at the source and transmitted along both the working and protection paths. The receiver is hence able to detect whether a failure occurs on the connections by extracting the CV packets. Additionally, connection selection does not influence the sending of CV packets. The default transmission period of CV packets for protection switching is 3.33 ms. According to [1], if no CV packets are received within an interval equal to 3.5 times the CV transmission period, a failure is assumed.

3.2 Carrier Ethernet Linear Protection

ITU recommendation G.8131 [2] defines two types of linear Carrier Ethernet protection: 1+1 and 1:1 trail protection. In 1+1 trail protection, which is illustrated in figure 5, a backup connection is dedicated to each primary LSP. In this hot-standby configuration, the traffic is permanently bridged to the working connection and protection connection at the source node. This means that the source node duplicates each packet and sends it on both the primary and the backup LSP. The sink node is then in charge of selecting from which path the packets should be used. This system has fast recovery times and is simple, but also expensive.

In the 1:1 protection case, as illustrated in figure 6, the traffic is transmitted on either the primary or the backup LSP. This means that in addition to the

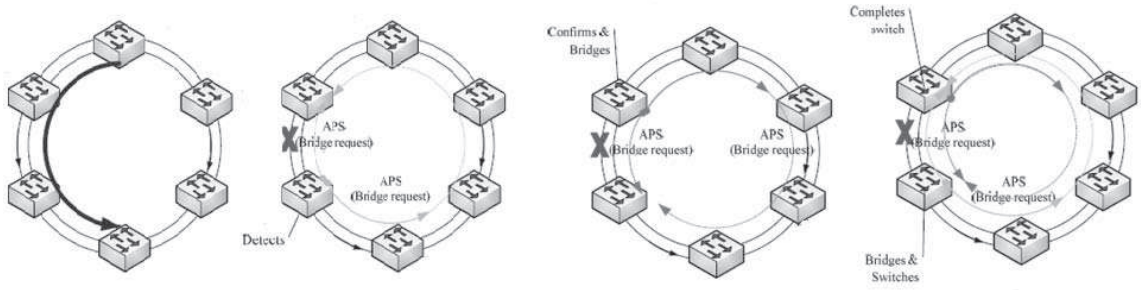

Figure 4: APS operation for Carrier Ethernet span failure.

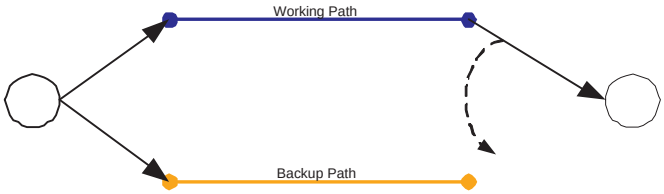

Figure 5: Carrier Ethernet 1+1 protection.

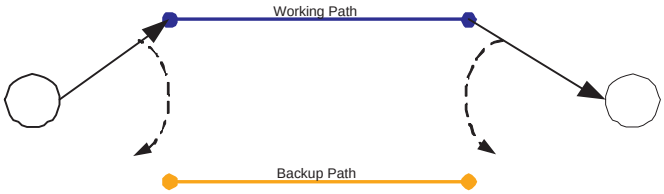

Figure 6: Carrier Ethernet 1:1 protection.

sink node, also the source node must participate in the selection process. This requires cooperation between the source and the sink selector, which can be achieved by using an Automatic Protection Switching (APS) protocol.

3.3 Carrier Ethernet Ring Protection

ITU-T has published a draft version G.8132 [3] which standardizes the APS process for T-MPLS shared protection ring recovery. Since this is only a draft version, the following section shows the operation of the APS protocol for T-MPLS shared ring protection when different failure types occur.

In figure 4, the failure of a span is illustrated, i.e. the fiber only fails in one direction. The challenge is then for the failure-adjacent nodes to detect the failure location and perform the switching action. Note that even if the fiber is not failed in the opposite direction, it is advisable to switch the connection to the backup path for both directions, since it eases the management. Detailed operation of the APS protocol and the related detection and bridging steps can be followed in figure 4.

In case of a node failure, the APS process is more complicated. This is due to the fact that the adjacent nodes can only see that there is a failure, but not if a node or the spans going to a node are affected. It should also be noted that the failure of an entire node is treated as a bidirectional failure. The failure and recovery process related to bridging actions is illustrated in figure 7.

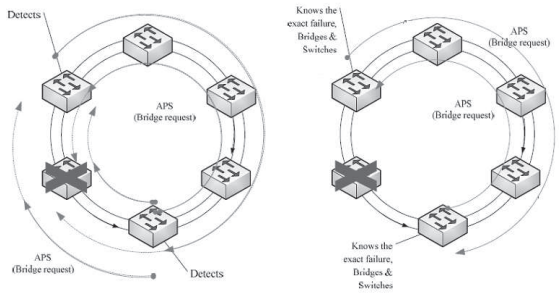

Figure 7: APS operation for Carrier Ethernet node failure.

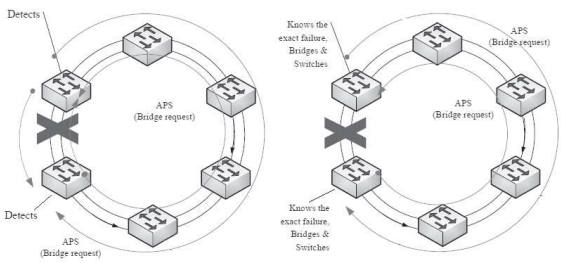

Figure 8: APS operation for Carrier Ethernet duct failure.

A duct failure means that all fibers between a node pair fail so that traffic transmission is impossible between the neighbors. It is another case of a bidirectional failure, thus the APS process is very similar to the case of a node failure. The two nodes adjacent to the failed duct send a bridge request in opposite directions to each other and receive the APS signal to get informed about the defect situation. Then the appropriate bridge and switch actions are performed, which is detailed in figure 8.

4 Simulation scenario and results

Previous studies [11, 12] show that the traffic availability and restorability can be significantly increased by applying appropriate resilience mechanisms to unicast traffic. To show the effect of protecting multicast traffic for IPTV distribution, some simulations have been carried out in OPNET SP Guru Transport Planner [10]. The simulated multi-ring topology is illustrated in figure 9. The multicasting tree, originating on node_0, is depicted with blue color.

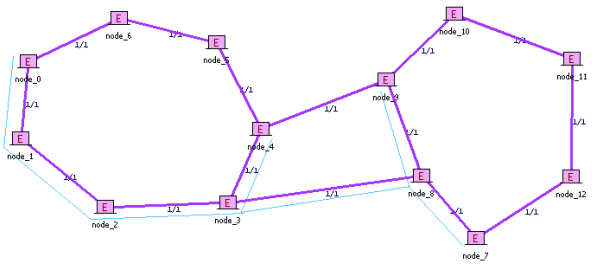

Figure 9: Investigated topology.

The following availability settings were used [7]:

- **Cables:** Cable length per cut per year = 300 km; MTTR = 24 h;
- **Nodes:** Mean Time Between Failures (MTBF) = 500'000 h; Mean Time To Repair (MTTR) = 24 h;

The results of the protection simulation are illustrated in figure 10. The simulation results show that a significant increase in the availability can be achieved if the multicast tree is protected. Even though the protection is costly, the gain may outweigh the cost of a break in the SLA and if good IPTV quality can be provided, a large amount of customers can be gained.

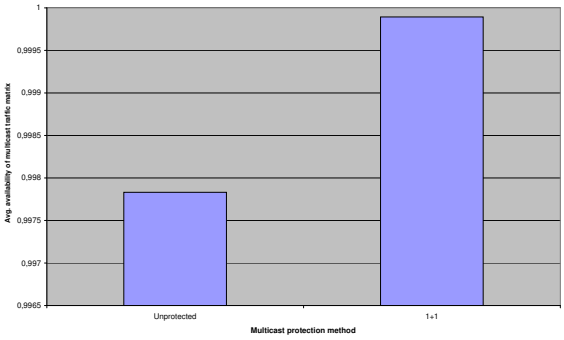

Figure 10: Availability of multicast traffic matrix.

5 Conclusion

In this paper, we presented an overview of the Carrier Ethernet technology. We go through the most important protocols in the field with specific focus on network resilience. We detail the protection methods in Carrier Ethernet linear and ring networks and outline the challenges for multicast resilience. Our simulation results show that the availability of the multicast tree can be significantly increased if resilience methods are applied, going. This shows that even though multicast protection is rather complex, the large gain in up-time justifies its application. This is particularly important for the providers of IPTV, for whom a breach in their SLAs can lead to severe economic punitive actions.

Acknowledgements: This research was supported by the Danish Advanced Technology Foundation (Hoejteknologifonden) through the research project HIPT.

References:

[1] ITU-T, Draft New Recommendation Y.17TOM, http://www.itu.int/ITU-T/

[2] ITU-T, Recommendation G.8131, Linear Protection, http://www.itu.int/ITU-T/

[3] ITU-T, Draft recommendation G.8132, Ring Protection, http://www.itu.int/ITU-T/

[4] MEF, Carrier Ethernet Overview, http://metroethernetforum.org/

[5] Carrier Ethernet: Its Attributes and Opportunities, http://whitepapers.zdnet.com/ abstract.aspx?docid=378400

[6] Ciena Whitepaper, http://www.wwp.com /resources/resources_whitepapers.htm?src=nav

[7] J.-P. Vasseur – M. Pickavet and P. Demeester, *Network Recovery, Protection and*

Restoration of Optical, SONET-SDH, IP, and MPLS, Morgan-Kaufmann Publishers Elsevier,2004,ISBN: 0-12-715051-x

[8] TPACK Whitepaper, PBT: Carrier Grade Ethernet Transport, http://www.tpack.com/resources/tpack-white-papers/pbb-te-pbt.html

[9] TPACK Whitepaper, Transport-MPLS: A New Route to Carrier Ethernet, http://www.tpack.com/fileadmin/user_upload/Public_Attachment/T-MPLS_WP_v1_web.pdf

[10] OPNET SP Guru Transport Planner, OPNET Inc., http://www.opnet.com

[11] S. Ruepp – J. Buron – N. Andriolli and L. Dittmann,*Nodal Stub-Release in All-Optical Networks*, IEEE Communication Letters, vol. 12, no. 1, pp. 47-49, Jan. 2008

[12] S. Ruepp – N. Andriolli – J. Buron – L. Dittmann and L. Ellegrd, *Restoration in All-Optical GMPLS Networks with Limited Wavelength Conversion*, Computer Networks Special Issue on Opportunities and Challenges in Optical Networks, vol. 52, no. 10, pp. 1951-1964, July 2008