Evaluating Multicast Resilience in Carrier Ethernet

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 gives an overview of the Carrier Ethernet technology with specific focus on resilience. In particular, we show how multicast traffic, which is essential for IPTV can be protected. We detail the background for resilience mechanisms and their control and we present Carrier Ethernet resilience methods for linear and ring networks. By simulation we show that the availability of a multicast connection can be significantly increased by applying protection methods.

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

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 [1] and T-MPLS [2], 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 [3] (T-MPLS linear protection switching with 1+1, 1:1 and 1:N versions) and G.8132 [4] (T-MPLS ring protection switching). Other resilience approaches have been treated in [5–11].

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. Section 3 introduces resilience concepts. In section 4 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, with explicit focus on the multicast situation. Section 5 presents our simulation study and the results. Section 6 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 [12].

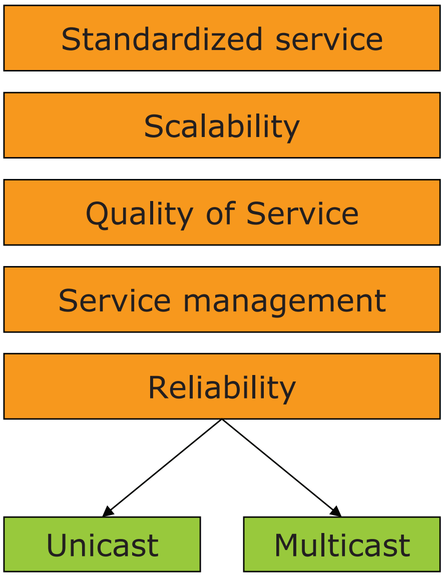


Figure 1: Metro Ethernet Forum requirements towards Carrier Ethernet.

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 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 [12].

Scalability Native Ethernet has limitations on scalability, which include the number of discrete users, MAC addresses, service connections, bandwidth options and L2VPN applications [13]. 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 [12].

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 [14].

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 Network Survivability

3.1 Failure Types

In an ideal world, communication services that have once been setup would continue running until they are no longer needed. Unfortunately, in real life networks failures do occur, and measures must be taken to ensure the continuation of communication services even when the network experiences failures. The traffic in a network can be affected by many kinds of failures, such as:

- Cable cuts
- Power failures
- Software bugs
- Hardware faults
- Fire
- Natural disasters
- Human errors

Cable cuts due to construction work cause the most significant number of network failures [15, 16].

But no matter the cause of the failure, the goal is the same: Communication networks must be able to survive faults - they must be resilient. A multitude of resilience mechanisms have been developed, and a representative selection of them is described in this section.

3.2 Basic Requirements

Some general requirements must be fulfilled to make a network resilient. The first requirement is dual homing, which requires that every node in the network must be connected to the rest of the network by at least two spans, else a single cable cut would separate the node from the rest of the network. The dual homing concept is illustrated in figure 2. There, if the span connecting the left-most node fails, the network is partitioned, whereas another span can be used in the dual homing case.

The second requirement does not allow the working (i.e. primary path) and backup paths to share the same physical route, i.e., they must be disjoint, else a single failure could take both the working path and the backup path out of operation. The two paths can either be span disjoint, meaning that they may not traverse any common spans; or they can be node disjoint where they may not visit the same nodes. An example of span and node disjointness is illustrated in figure 3. Disjointness can be ensured by categorizing network elements into SRLG, which define fate sharing, which means that a single failure can result in the failure of all elements within the same SRLG. By taking SRLG into account in the route calculation, a working and a and backup path that cannot be affected by the same single failure, can be chosen.

The availability of a network element is used to describe the probability that it is operational at some point in time [17]. The availability A is calculated according to equation 1, where $MTTR$ denotes the mean time to repair and $MTBF$ the mean time between failures of a network element.

$$A = 1 - \frac{MTTR}{MTBF} \qquad (1)$$

The availability of a network can be calculated according to equation 2, provided that independence of failures is assumed [17]. $A_{Network}$ is the network availability and $A_1 ... A_n$ are the availabilities of each of the network elements.

$$A_{Network} = A_1 \cdot A_2 \cdot ... \cdot A_n \qquad (2)$$

Decreasing the failure occurrence (i.e., $MTBF$) has a direct effect on the availability of a network and it is therefore desirable to minimize it. This can be done by making some of the node equipment redundant, e.g., the power supply, or by digging the cable deeper into the ground. Despite these measures failures cannot be avoided completely and therefore it is necessary to anticipate them and provide a plan of action for traffic recovery. This is achieved by so-called network recovery or resilience schemes, which operate at a network scale level. The basic idea of network recovery is to divert traffic onto functioning backup paths in case of a failure. As soon as a failure is detected, the recovery mechanism automatically diverts the traffic that is affected by the failure from the working path to the backup path [18].

3.3 Criteria for Recovery Method Evaluation

With many recovery methods to choose from, the question of which one is better naturally emerges. To compare the methods, it is necessary to have some common criteria. These criteria include:

- Recovery percentage
- Capacity usage
- Operational complexity
- Recovery speed
- Node resource usage

The most common approach is to evaluate recovery methods under a single span failure assumption. If a single node failure is assumed, it can be treated as the failure of all spans connected to that node.

3.4 Fault Management

The first step in successful connection recovery is to detect that there has been a failure. It takes some time for the failure adjacent nodes to notice a fault, identify exactly which component has failed, and notify the entity responsible for fault management. When a failure is suspected, the system moves to a hold-off state to make sure that recovery is only initiated at persistent fault conditions, and also to give techniques of other layers a chance to recover from the failure. If the hold-off period expires and the failure persists, its exact location must be determined to initiate proper recovery actions, circumventing the failed element(s). It is possible that a single failure causes several fault indications. Therefore, to decrease the signaling overhead, the fault indications are correlated before they are dispatched to the node that initiates the connection recovery. received, the actual connection recovery is initiated.

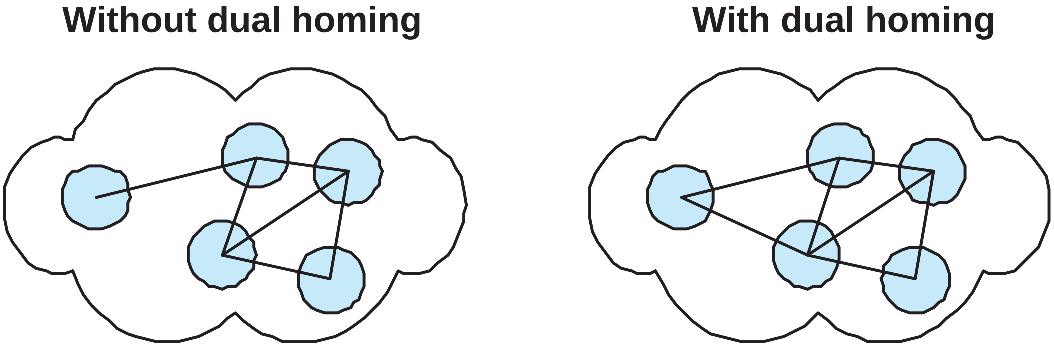


Figure 2: Dual homing example.

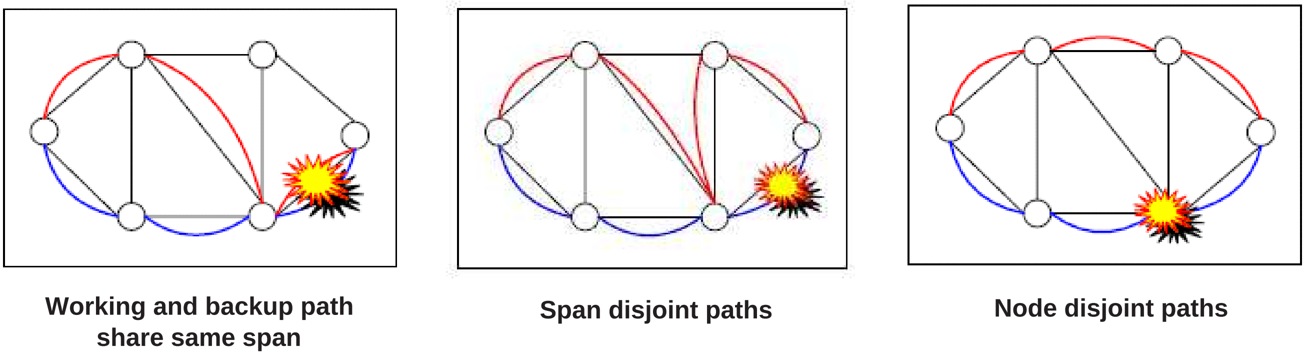


Figure 3: Span and node disjointness.

3.5 Protection vs. Restoration

In the field of network survivability the two terms protection and restoration are widely used. Although both methods are used to ensure that the traffic is switched to a backup path in case of a failure, there is a subtle difference between them, which is related to when the backup resources are provisioned.

Protection refers to the situation where the backup path is provisioned when the working path is set up. Everything is calculated before the failure occurs: the route, which resources to use, and the switches are configured. This means that when a failure occurs, the backup path is ready for the traffic, ensuring fast and guaranteed traffic recovery. The main drawback of protection is its static nature due to the fact that recovery paths are pre-planned. Therefore, protection can only recover from failures that were anticipated (e.g., a single span failure); if something unforeseen happens the traffic cannot be recovered.

Restoration describes the situation where a spare capacity pool is available in the network instead of pre-assigned backup capacity. In contrast to protection, a connection does not reserve spare capacity when the primary path is provisioned. Only when a failure occurs, a suitable backup path is identified and the necessary resources are reserved. Hence, a restoration scheme allows for more flexibility than a protection scheme when dealing with unexpected failures, because there is often more than one possible restoration path. But since the search for a restoration path only starts when a failure occurs, the recovery time is longer for restoration than for protection. There exist several sub-categories of restoration, depending on whether they contain an element of pre-planning. In so-called pre-planned restoration [19] a set of recovery paths are pre-calculated, but not provisioned until after the failure. This is beneficial for the recovery time if an anticipated failure occurs; else path re-computation is required as well.

Restoration is applied in mesh networks, where the high density allows for several recovery path alternatives. Therefore, span, path and segment protection (which are described in the following sections) also exist in their respective restoration versions.

Protection and restoration can also be combined within the same network, e.g., protection for the most important traffic and restoration for other traffic. This can be used to provide differentiated resilience [20]. Furthermore, restoration can be applied in case protection cannot resolve a given failure situation, e.g., a dual failure affecting both the working and backup path of a protected connection [18].

Further details on the recovery methods can be found in [16–19, 21].

4 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 4 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.

- 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.

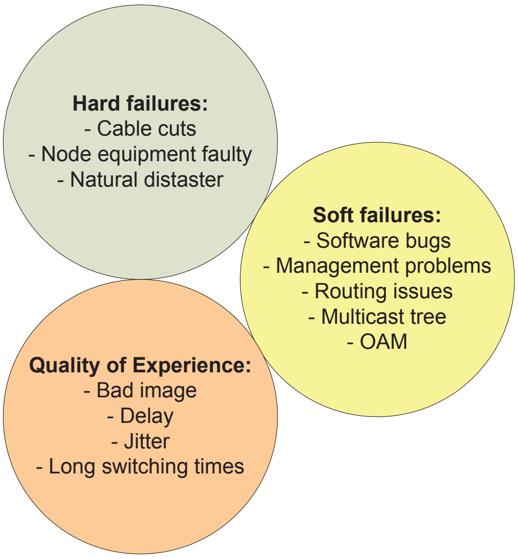


Figure 4: Failure types.

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

4.1 Failure detection in Carrier Ethernet

The OAM protocol is used to detect failures of the primary or backup LSPs. According to [22], 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 [22], if no CV packets are received within an interval equal to 3.5 times the CV transmission period, a failure is assumed.

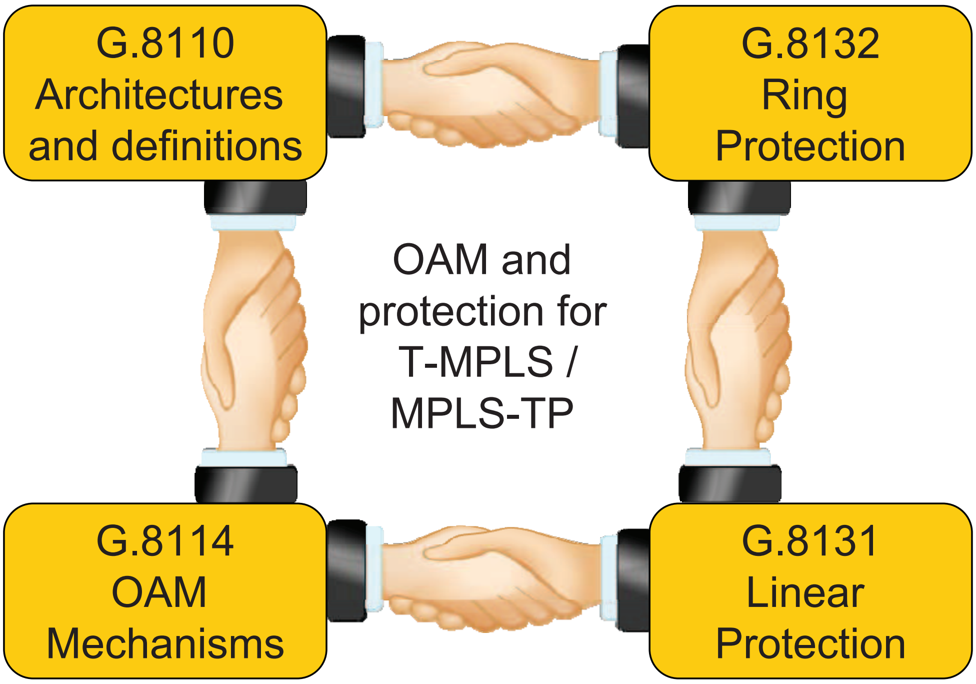
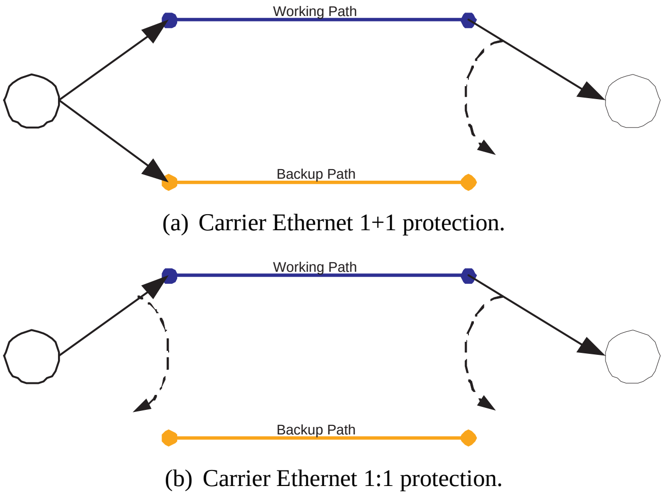


Figure 5: OAM and protection for T-MPLS/MPLS-TP.

4.2 Carrier Ethernet Linear Protection

ITU recommendation G.8131 [3] 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 7(a), 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.

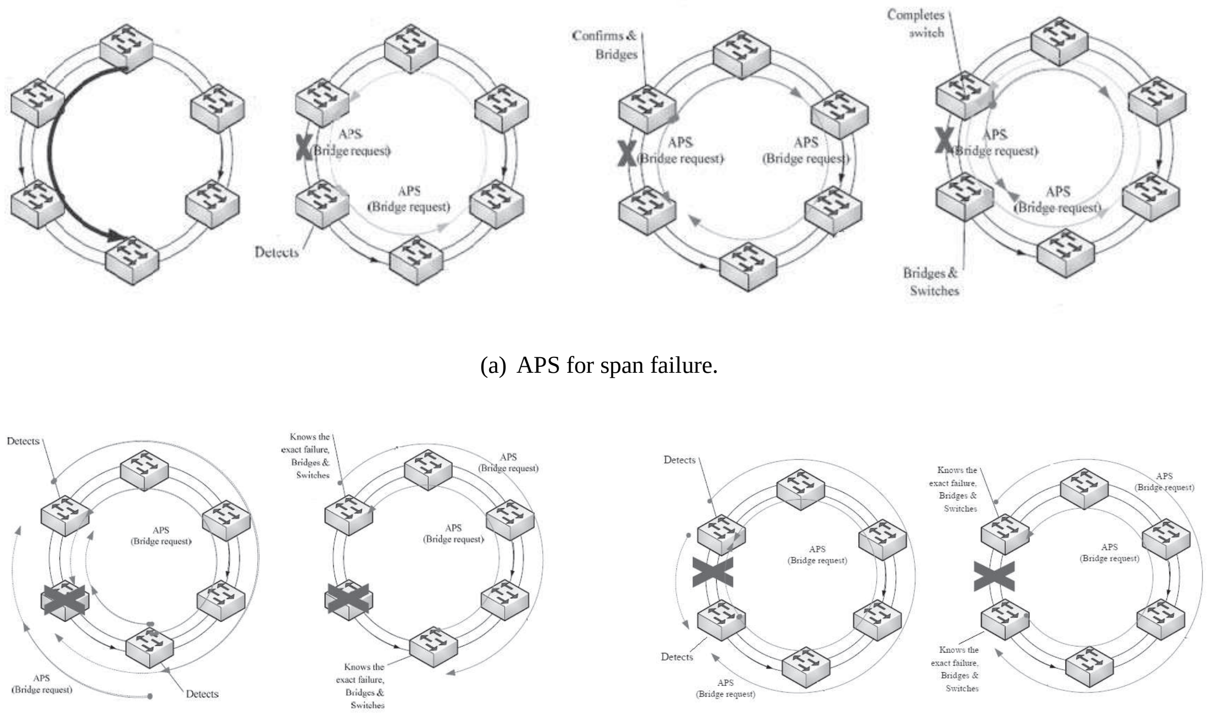
In the 1:1 protection case, as illustrated in figure 7(b), the traffic is transmitted on either the primary or the backup LSP. This means that in addition to the sink node, also the source node must participate in the selection process. This requires cooperation between the source and the sink selector, which can be achieved by using an Automatic Protection Switching (APS) protocol.



(a) Carrier Ethernet 1+1 protection.

(b) Carrier Ethernet 1:1 protection.

Figure 7: Carrier Ethernet protection.



(a) APS for span failure.

(b) APS for node failure.

(c) APS for duct failure.

Figure 6: APS operation for Carrier Ethernet failure location types.

4.3 Carrier Ethernet Ring Protection

ITU-T has published a draft version G.8132 [4] 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 6(a), 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 6(a).

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 6(b).

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 6(c).

5 Simulation scenario and results

Previous studies [5, 6] 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 [23]. The simulated multi-ring topology is illustrated in figure 8. The multicasting tree, originating on node_0, is depicted with blue color.

The following availability settings were used [18]:

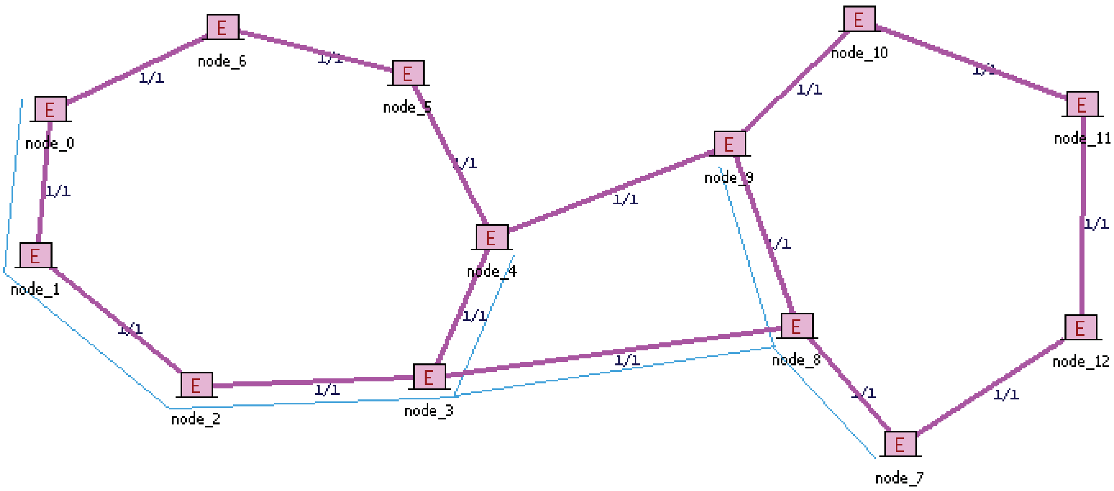


Figure 8: Investigated topology.

- **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 9. 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.

6 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 projects HIPT and 100 GE.

References:

[1] “Tpack whitepaper, pbt: Carrier grade ethernet transport.” [Online]. Available: http://www.tpack.com/resources/ tpack-white-papers/pbb-te-pbt.html

[2] “Tpack whitepaper, transport-mpls: A new route to carrier ethernet.” [Online]. Available: http://www.tpack.com/fileadmin/user_upload /Public_Attachment/T-MPLS_WP_v1_web.pdf

[3] International Telecommunication Union (ITU-T), “Draft recommendation G.8131, linear protection.” [Online]. Available: http://www.itu.int/ITU-T/

[4] ——, “Draft recommendation G.8132, ring protection.” [Online]. Available: http://www.itu.int/ITU-T/

[5] S. Ruepp, J. Buron, N. Andriolli, and L. Dittmann, “Nodal stub release in all-optical networks,” *IEEE Commun. Lett.*, vol. 12, no. 1, pp. 47–49, Jan. 2008.

[6] S. Ruepp, N. Andriolli, J. Buron, L. Dittmann, and L. Ellegard, “Restoration in all-optical GMPLS networks with limited wavelength conversion,” *Computer Networks Special Issue on Op-*

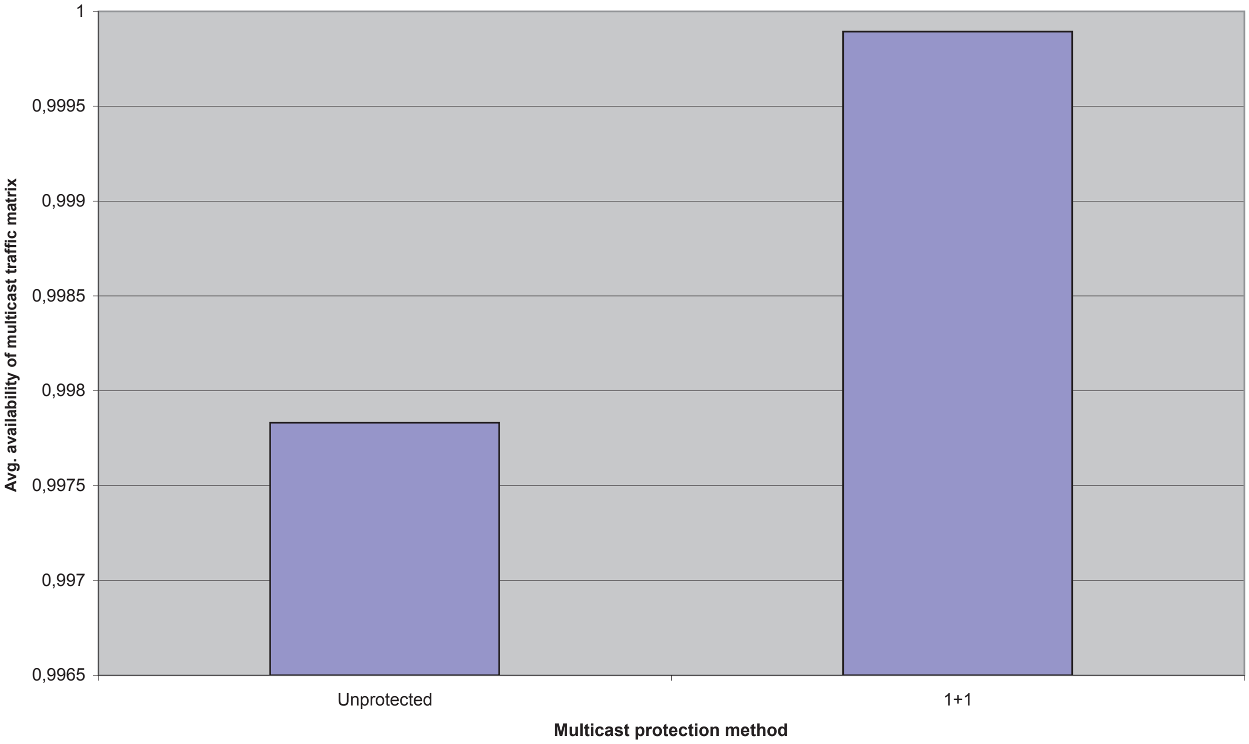


Figure 9: Availability of multicast traffic matrix.

portunities and Challenges in Optical Networks, 2008.

[7] K. Kim and B. Yae, "Protection switching scheme for ng-sdh based switching system," *WSEAS TRANSACTIONS on SYSTEMS*, 2006.

[8] S. Prahmkaew and C. Jittawiriyanukoo, "Approximation approach of adaptive rate control (arc) with erlangian telecommunication traffics over resilient packet ring (rpr) network," in *WSEAS TRANSACTIONS on COMPUTERS*, vol. 5, March 2006.

[9] A. Azadmanesh, A. Krings, and D. Laqab, "Multicast survivability in hierarchical broadcast networks," in *WSEAS TRANSACTIONS on COMMUNICATIONS*, vol. 7, 2008.

[10] A. Sierra, N. Kolothody, and S. V. Kartalopoulos, "Cas and gfp for service protection in next generation sonet/sdh," in *Proceedings of the 9th WSEAS International Conference on Communications*, 2005.

[11] S. RUEPP, H. WESSING, J. ZHANG, A. V. MANOLOVA, A. RASMUSSEN, L. DITTMANN, and M. BERGER, "Providing resilience for carrier ethernet multicast traffic," in *Proc. CISST Conference at Harvard University*, 2010.

[12] M. E. F. MEF, "Carrier ethernet overview." [Online]. Available: http://metroethernetforum.org/

[13] "Carrier ethernet: Its attributes and opportunities." [Online]. Available: http://whitepapers.zdnet.com/ abstract.aspx?docid=378400

[14] "Ciena whitepaper." [Online]. Available: http://www.wwp.com /resources/resources_whitepapers.htm?src=nav

[15] TDC Pressesekretariat, "Flere kabler graves over," cited: 3. June 2005. [Online]. Available: http://www.tdc.dk

[16] B. Mukherjee, *Optical WDM Networks*. Springer, 2006, ISBN: 0-387-29055-9.

[17] A. Farrel and I. Bryskin, *GMPLS Achitecture and Applications*. Morgan Kaufmann, Elsevier, 2006, ISBN: 0-12-088422-4.

[18] 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.

[19] W. Grover, *Mesh-Based Survivable Networks - Options and Strategies for Optical, MPLS, SONET, and ATM Networking*. Prentice-Hall, 2004, ISBN: 0-13-494576-X.

[20] S. Dong, C. Phillips, and R. Friskney, "Differentiatedresilience provisioning for the wavelengthrouted optical network," *J. Lightw. Technol.*, vol. 24, no. 2, pp. 667–673, Feb. 2006.

[21] G. Bernstein, B. Rajagopalan, and D. Saha, *Optical Network Control - Architecture, Protocols and Standards*. Boston, USA: Pearson Education Inc., 2004, ISBN: 0-20-175301-4.

[22] International Telecommunication Union (ITU-T), "Draft new recommendation Y.17TOM." [Online]. Available: http://www.itu.int/ITU-T/

[23] "OPNET SP guru transport planner, OPNET technologies, inc." [Online]. Available: http://www.opnet.com