

Ethernet Operation Administration and Maintenance *Opportunities for the NREN community*

Mark Prins¹, Richa Malhotra²

1: TNO, P.O. Box 5050, 2600 GB Delft, The Netherlands, Email: mark.prins@tno.nl

2: SURFnet, P.O. Box 19035, 3501 DA Utrecht, The Netherlands, Email: richa.malhotra@surfnet.nl

Paper type

Technical paper

Abstract

Ethernet started its life as a Local Area Network technology and initially did not have Operations, Administration and Maintenance (OAM) features like IP Ping, IP Traceroute and SDH Loss of Frame. Monitoring and management was mainly done on the IP level. In the case of delivery of Ethernet connections or services IP OAM traffic could follow a completely different path through the networks than the end user traffic going through the Ethernet connection or service. This is clearly not desirable if end-to-end connections or services have to be monitored through the network. Fortunately, in the last years several standardization bodies like IEEE, ITU and MEF have extended Ethernet with carrier grade OAM features which address the aforementioned issue. With the increasing penetration of Ethernet based services worldwide including the NREN community, these OAM features could prove extremely beneficial in terms of diagnosing the network, monitoring services and verifying their performance end-to-end. This paper shortly describes several Ethernet OAM mechanisms and considers several useful intra- and inter-NREN network deployment scenarios of these mechanisms. Ethernet OAM seems the homogeneous technology of choice to use in multi NREN domain Ethernet service delivery monitoring. The value of the use of Ethernet OAM in single domain Ethernet service monitoring is highly dependant on the dominant Ethernet transport technology used in the NREN domain. The results of this paper can be used as a starting point when planning to deploy monitoring for Ethernet services in a single and multi domain environment.

Keywords

Ethernet, OAM, Carrier Ethernet, multi domain, network management

1. Introduction

Ethernet has been prevalent in many NREN networks for some years now, mostly providing aggregation functionality for IP services. However, due to recent advances in the technology and its global uptake, it is being considered as a basis for circuit and lightpath services as well. The lightpaths in the next generation SURFnet network, SURFnet7, are even expected to take a step further and be transported over Carrier Ethernet technology. At the same time dynamic lightpaths are not lagging behind. Pilot projects like the Automated GOLE project [1] are investigating as well as promoting the set-up of dynamic circuit services based on Ethernet VLANs.

In view of these emerging trends, the advancements in Ethernet are being investigated in multiple projects within the NREN community. The Gigaport3 project [2] at SURFnet as well as the GN3 project [3] are addressing various aspects associated with Carrier Ethernet. As part of JRA1 T1, technology testing of Carrier Ethernet will be carried out in intra and inter domain networks. The topic of Operations, Administration and Maintenance (OAM) with a special focus on performance monitoring at the Ethernet layer is being addressed as part of JRA2 T3, as these mechanisms provide specific opportunities for an end-to-end performance monitoring infrastructure like perfSONAR.

In this paper we provide a short overview of Ethernet OAM mechanisms. Further in the paper we enlist relevant service and network monitoring scenarios both within an NREN domain as well as over multiple NREN boundaries. The paper is concluded by identifying promising scenarios as well as open issues which still need attention and communication among various NREN operators.

2. Ethernet OAM

Ethernet started its life as a Local Area Network technology [4]. Monitoring was mainly done on the IP level. Ethernet did not have Operations, Administration and Maintenance (OAM) features like IP Ping, IP Traceroute and SDH Loss of Frame. The consequence of using IP layer OAM techniques for an Ethernet network is that the OAM traffic can end up following a completely different path than the actual data traffic. This is highly undesirable when monitoring the end-to-end performance of an Ethernet service. In order to overcome this issue several standardization bodies like IEEE, ITU and MEF have extended Ethernet with carrier grade OAM features. Although Ethernet OAM originated from requirements in the Carrier Ethernet environment, the use of Ethernet OAM is not limited to Carrier Ethernet and can be used for standard switched Ethernet networks as well.

Further in this paper we will refer to an end-to-end Ethernet service as an Ethernet Virtual Connection (EVC). The EVC can be a service by itself or used to transport a lightpath or an IP service.

As depicted in Figure 1 the level on which Ethernet OAM is delivered can be split into three categories.

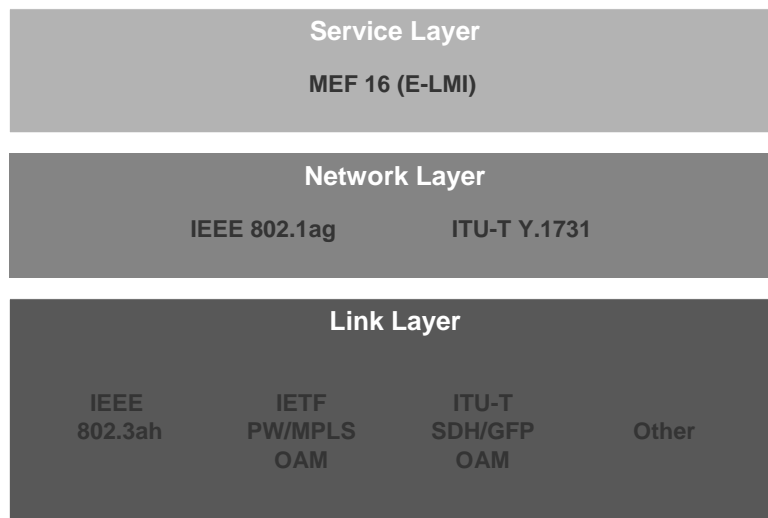


Figure 1: Three layers of OAM

- **Link layer OAM** : Monitors and manages the link between two devices. For Ethernet the IEEE formulated the 802.3ah standard [5]. This standard includes mechanisms like discovery and remote loopback.
- **Network layer OAM**: It is also sometimes referred to as Service layer OAM, and is used to monitor and troubleshoot end-to-end EVCs and their intermediate nodes. Two similar but also partly complimentary toolsets have been defined by the IEEE and the ITU: IEEE 802.1ag [6] and ITU-T Y.1731 [7] respectively. Mechanisms defined by these standards include continuity checks, link traces and remote defect indication.
- **Service Layer OAM**: For Ethernet management from the network to the customer domain the Metro Ethernet Forum has formulated the Service layer MEF E-LMI specification [8]. The specification defines mechanisms to signal the EVC status from the network edge to the customer and to configure and provision Customer Premises Equipment remotely.

3. OAM mechanisms

3.1 Link layer – IEEE 802.3ah

As stated IEEE 802.3ah operates on the link layer. This means 802.3ah frames are never forwarded by Ethernet devices (bridges, switches). Instead they are handled and acted upon by the OAM process in the Ethernet devices. IEEE 802.3ah defines six OAM functions: Discovery, link monitoring, remote failure indication, remote loopback, MIB variable retrieval and the possibility for organization specific extensions.

The *Discovery* function is used to discover connected IEEE 802.3ah-enabled nodes and to learn of their capabilities.

The *Link monitoring* function can detect and signal link failures. For instance it can inform remote nodes about the number of errored frames.

Where link monitoring informs remote nodes about failures on their interlinks *Remote failure indication* is used to inform remote nodes on failures in nodes like power failures.

Remote loopback is used to put a remote node in loopback to test full duplex communication of a link using test traffic.

To request values of a remote nodes MIB the *MIB variable retrieval* function of IEEE 802.3ah can be used.

The *Organization specific extensions* make it possible for vendors to extend the functionality of 802.3ah with additional messages.

3.2 Network layer – IEEE 802.1ag and ITU-T Y.1731

Where IEEE 802.3ah only considers the link between two Ethernet nodes IEEE 802.1ag and ITU-T Y.1731 specify functions to manage end-to-end Ethernet services (EVCs).

Both specifications partly describe the same functionalities, but the ITU-T specification stretches a bit further by defining some extra functionalities including performance management. Table 1 and Table 2 show the functionalities – fault and performance management – that are specified by the two standards and what functions are used to fill in these functionalities.

	IEEE 802.1ag	ITU-T Y.1731
Fault Detection	Continuity Check	Continuity Check
Fault Verification	Loopback	Loopback
Fault Isolation	Link-Trace	Link-Trace
Fault Notification	Remote Defect Indication	Alarm Indication Signal Remote Defect Indication
Fault Recovery	<i>Not included in this standard</i>	Automatic Protection Switching

Table 1: Fault management functions

	IEEE 802.1ag	ITU-T Y.1731
Frame loss ratio	<i>Not included in this standard</i>	Loss Measurement
Frame delay	<i>Not included in this standard</i>	Delay Measurement
Frame delay variation	<i>Not included in this standard</i>	Delay Measurement
Throughput	<i>Not included in this standard</i>	Loopback or Test

Table 2: Performance management functions

Fault Detection is implemented by *Continuity Check* (CC) messages that are sent periodically from edge nodes from the management domain. These edge nodes are called Maintenance association End Points (IEEE 802.1ag) or Maintenance entity group End Points (ITU-T Y.1731) (MEPs). These messages are multicasted within the management domain and in normal situations received by all the other MEPs in the domain. Figure 2 illustrates this process. When CC messages from a MEP are not received within a certain interval this can indicate a failure.

With information about CC messages from all the MEPs it is possible to do a first step in the isolation of the fault.

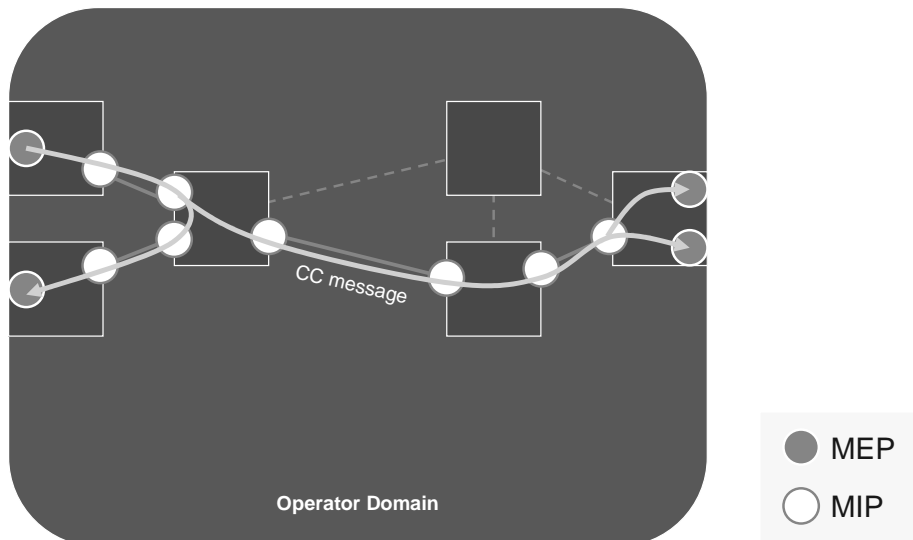


Figure 2: Continuity Check function

When a fault is detected the next step is to verify the fault. For *Fault Verification* the standards have implemented a *Loopback* function. This function is comparable to the ICMP Echo function in IP networks. The Loopback function is initiated on-demand. A Loopback (LB) message is sent from a MEP or MIP (Maintenance association Intermediate Point) destined for a remote MIP or MEP. On receiving this message the remote MEP or MIP replies with a Loopback reply message. Figure 3 shows this process.

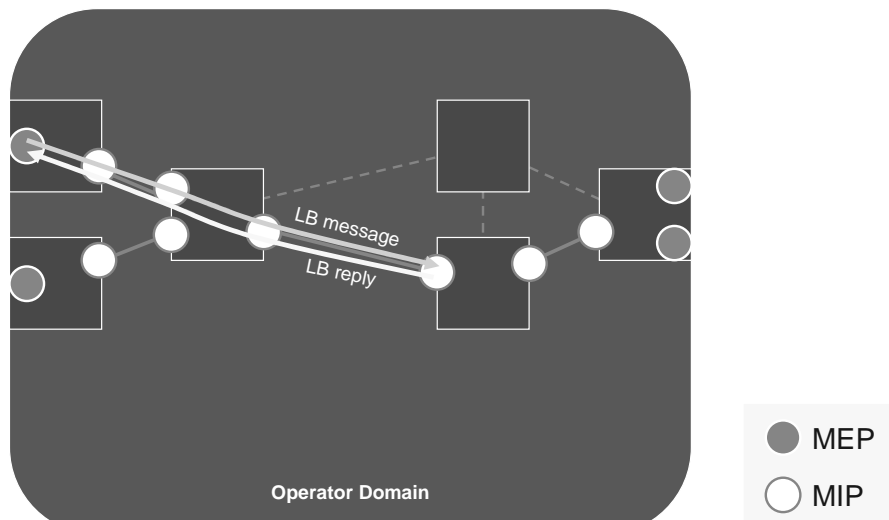


Figure 3: Loopback function

When the fault is verified it is time to isolate the failure. Just like in IP networks Ethernet OAM implements a *Link-Trace* function for *Fault Isolation*. In IP networks the functionality is based on ICMP Echo messages sent with increasing TTL (Time To Live) values. Because Ethernet does not have this TTL functionality the Link-Trace function of Ethernet OAM is based on dedicated Link-Trace (LT) messages and relies on the intermediate nodes to respond to these messages destined for the remote node. The process is illustrated in Figure 4.

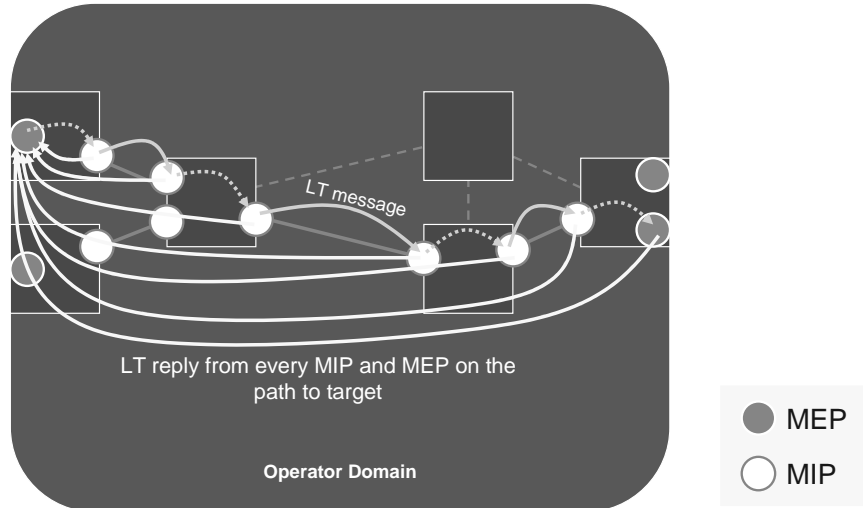


Figure 4: Link-Trace function

For fault management ITU-T also defines *Fault Notification* and *Fault Recovery* functions. *Fault Notification* is implemented by *Alarm Indication Signal* and *Remote Defect Indication* where the first is used to inform maintenance domains on a higher level of a failure in the underlying domain(s). The second is used to inform nodes of a failure in a remote node in the same maintenance domain. Remote Defect Indication is also included in the IEEE 802.1ag specification.

Fault Recovery is supported by ITU-T Y.1731 by means of the specification of an *Automatic Protection Switching* message. The exact usage of this message is out of the scope of the Y.1731 specification. Applications of this message are defined in ITU-T G.8031 [9].

Next to fault management the ITU-T Y.1731 standard also specifies some performance management functions. These functions are *Loss Measurement* and *Delay Measurement* – used for delay and delay variation measurements – and *Throughput* measurements implemented by using the already existing *Loopback* and *Test* messages. These performance management functions are at this moment only specified for point-to-point EVCs (E-LINE).

4. Deployment scenarios

In our study we have considered several scenarios in which the different categories of Ethernet OAM could be applied and provide benefits for NRENs. These scenarios are enlisted below.

- The considered scenarios include monitoring of the connectivity and performance of EVCs in a single NREN domain.
- Also the multi NREN domain situation is considered.
- Scenarios are also investigated in which customers can get insight in the status of their EVCs by enabling Ethernet OAM on specific nodes in the NREN networks.
- The last scenario outlines the possibility (for customers) to generate Service Level reports in order to verify conformance of the actual service delivered by the network to the prespecified Service Level Agreement.

In the next four Sections the different deployment scenarios will be further elaborated upon and a view on the usefulness of different Ethernet OAM functions is given.

4.1 Single domain

The first scenario is a scenario where Ethernet OAM is used to monitor and troubleshoot the network of one operator/NREN. Figure 5 shows an example of an Ethernet circuit in an operator domain with the accompanying MEPs and MIPs.

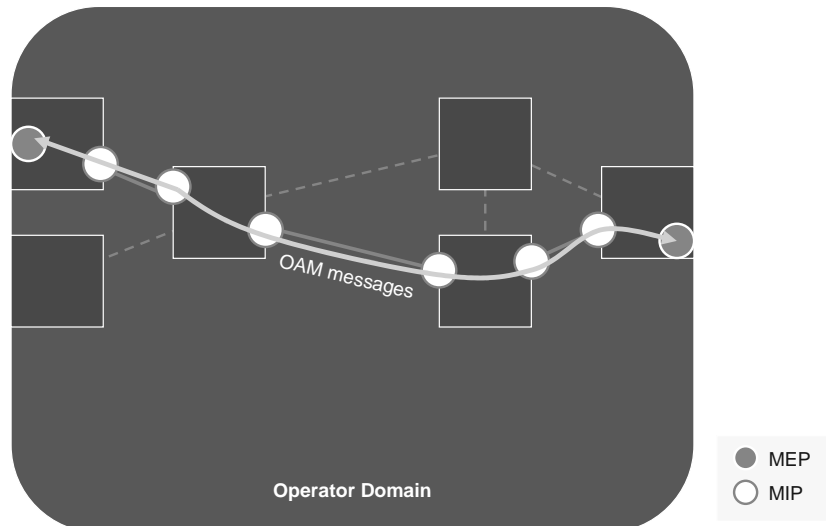


Figure 5: Single domain OAM

Typically network layer OAM would be used to monitor the end-to-end Ethernet circuit in the operator domain. End-to-end circuits in this sense are multi node paths through the transport network of the NREN. Network layer OAM can be assisted by link layer OAM between nodes. The type of link layer OAM used will depend on the underlying technologies used.

As discussed in the previous Chapter network layer OAM can be used for different fault and performance management tasks.

One of the most important fault management functions is fault detection implemented by Continuity Check messages automatically and periodically sent and received by MEPs. For fault detection purposes a recommended interval between CC messages would be 1 second. This would mean a failure in an Ethernet circuit could be detected within 3.5 seconds.

When the CC messages would be used to enable protection switching of Ethernet circuits a shorter interval of the messages is desired. An example of such an application is in the IEEE 802.1Qay standard also known as PBB-TE. The recommended interval (according to [7]) in such a situation would be 3.3 milliseconds (300 frames/second). This would lead to a failure detection time of less than 12 milliseconds and should provide a possible switchover time of less than 50 milliseconds. When this approach is used for all EVCs provisioned on the network this could potentially lead to a substantial load on the network. See also Table 22-3 and 22-4 in [6].

On-demand use of fault verification and isolation implemented by Loopback and Linktrace messages can be used in case a failure occurs in the network. MIPs configured on nodes in the network can give insight in whether and where a failure has occurred in the network. The more nodes have MIPs configured the higher the granularity of failure localisation you can get.

Next to fault management tasks Ethernet OAM can be used to periodically monitor the performance of the NREN network. End-to-end probes as defined by [7] can give a clear insight in the quality of the service that is delivered to end users.

As explained earlier when several EVCs are transported over the same transport path in a network the added overhead of several Continuity Check messages travelling the same path can lead to an unnecessary high load on the transport links. This is especially the case when these messages are sent on a high frequency (> 10 frames/second). When your OSS and BSS system stores a clear relation between transport path (e.g. MPLS LSP) and the customer Ethernet service (EVC) OAM on the transport layer could trigger the OSS/BSS to display a failure on all the affected upper EVCs more efficiently.

Ethernet OAM can be useful in the single domain situation but then especially in the cases Ethernet is the dominant transport technology (e.g. PBB-TE). In other cases (e.g. MPLS based networks) other transport technology related OAM mechanisms can prove to be more beneficial.

4.2 Multi domain

It is not uncommon for data connections for research activities to span more than one NREN domain. These data connections can be interconnected between NRENs on the IP, lightpath and – with the rise of Ethernet as carrier grade transport technology – on the Ethernet level. To monitor and troubleshoot the latter multi domain Ethernet connections (EVCs) network layer OAM can be used. Figure 6 shows a deployment example of a multi NREN domain EVC. If the provider domain as depicted in the figure exists it could be a purely administrative role operated by a separate company or one of the two involved NRENs.

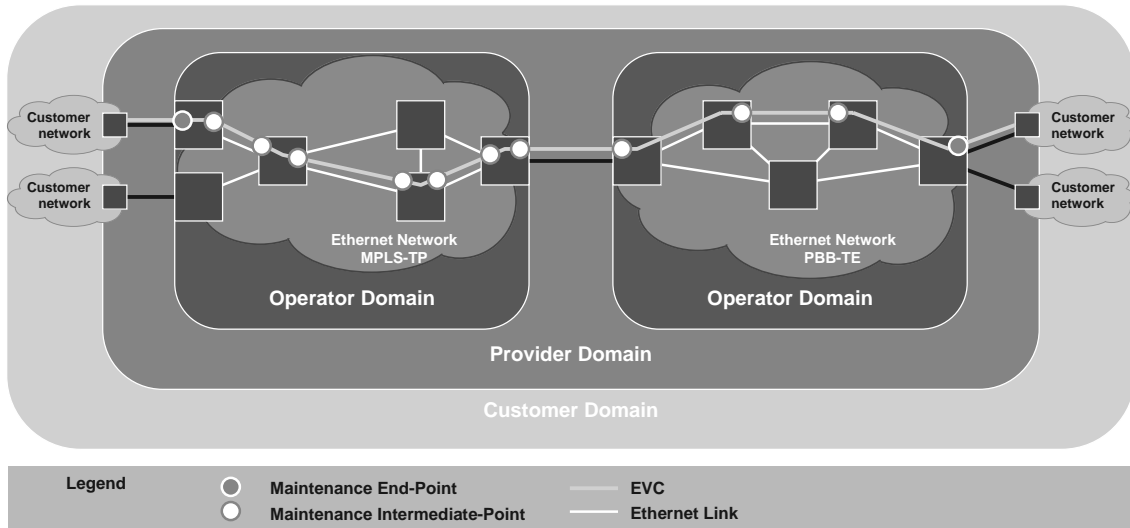


Figure 6: Multi domain OAM

The multi domain network layer OAM can be used in addition to the network layer OAM used in the single NREN domain situation. For instance it extends the monitoring capabilities with the possibility to detect failures of network nodes in neighbouring NRENs. It gives the possibility to monitor the status of end points of Ethernet services delivered over multiple operator domains. The status of all end points can be monitored even when some of the end points are not situated in your network.

Next to fault detection network layer OAM could also be very beneficial for fault verification and isolation in multi NREN domain Ethernet services. It provides the ability to give (partial) insight in the network of neighbouring NRENs to aid troubleshooting. Because it is possible to selectively configure MIPs on the network nodes it is possible to control the amount of insight that is given in the network.

Just as was the case for the single domain scenario in the multi domain scenario performance management functions can give insight in the service quality that is delivered on EVC level.

Because NRENs can use different transport technologies to deliver the EVC services Ethernet OAM on the EVC level seems the ideal technology to monitor and troubleshoot multi-domain EVCs. For instance one of the two NRENs in Figure 6 uses MPLS-TP to transport the EVC, but the other NREN uses the purely Ethernet-based PBB-TE.

In network layer OAM to distinct between OAM messages related to your own domain only and messages sent over multiple domains the concepts 'Maintenance Domain' and 'Maintenance Domain (MD) Level' are used. MD level is defined by an integer value (0-7) in an OAM message frame indicating Maintenance Points (MEPs and MIPs) interested in its contents and through which Maintenance Points it may flow. A Maintenance Domain is a collection of MEPs, at the same MD Level and belonging to the same administration, serving one or more EVCs. Figure 7 shows the relation between MD levels and Maintenance Domains. The different MD levels make it possible to define different Maintenance Domains that are nested.

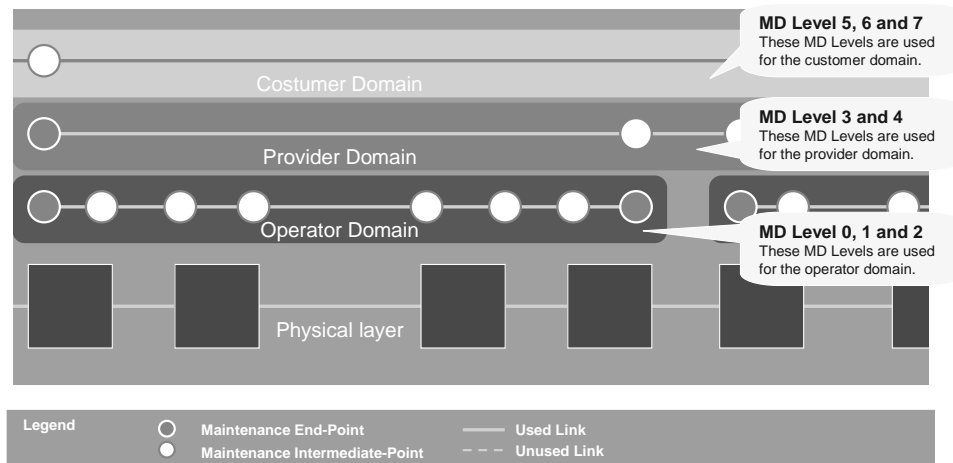


Figure 7: Maintenance Domains and Maintenance Domain Levels

As discussed Ethernet OAM can be very beneficial in monitoring and troubleshooting of multi NREN domain Ethernet services, but before these multi domain capabilities can be deployed in an NREN environment some important aspects need to be negotiated between the interconnecting NRENs.

Some of the aspects to take into consideration are:

- Decide on what functions (Fault detection, fault isolation, etc) to support and according to which standard. As discussed several functions are standardised by different standardisation bodies. NRENs should negotiate which of these functions to use in multi domain scenarios.
- Decide on the place of Maintenance Domain boundaries and the MD levels and Maintenance Association Identifiers (MAID) to be used. For the end-to-end OAM messages to flow correctly and be identified and interpreted correctly it is crucial to communicate amongst NRENs where the Maintenance Domain boundaries will be situated and to align the MD levels and MAIDs to be used.
- Decide on which nodes to appoint as MEP. This is dependant on the placement of the Maintenance Domain boundaries (b) and the OAM functions to support (a).
- Decide on the amount of insight you will give in your network. In other words: Decide which nodes will be made MIPs in the Maintenance Domain. NRENs should negotiate which points in their networks will be visible to the others to most efficiently and effectively support the troubleshooting of multi NREN domain EVCs.
- Decide the values that will be used for the different OAM parameters. This includes for instance Continuity Check message intervals. When these values are not properly aligned wrong conclusions can be drawn from the resulting OAM triggers.

When delivering Ethernet services spanning several NREN domains Ethernet OAM seems to be the most promising homogeneous technology to maintain these services.

4.3 Customer insight

Where the first two scenarios were focussing on the maintenance of Ethernet services by the operators and providers this third scenario is especially focussed on the fault verification and isolation possibilities for customers of EVC services. By enabling Maintenance Intermediate Points in the intermediate NREN networks the customer can get a sense of where a failure might have occurred in the network and can approach the point of contact for the domain the failure is occurring immediately.

Customers to switch their traffic between primary and secondary EVCs could also use Ethernet OAM on this level to trigger this. These EVCs could for instance be delivered via different NREN paths.

Just like in the multi-domain scenario some decisions have to be made and some things have to be negotiated. For instance a decision has to be made on the placement of the MIPs which determine the amount of insight you give in the network.

Figure 8 depicts a deployment example of such a scenario.

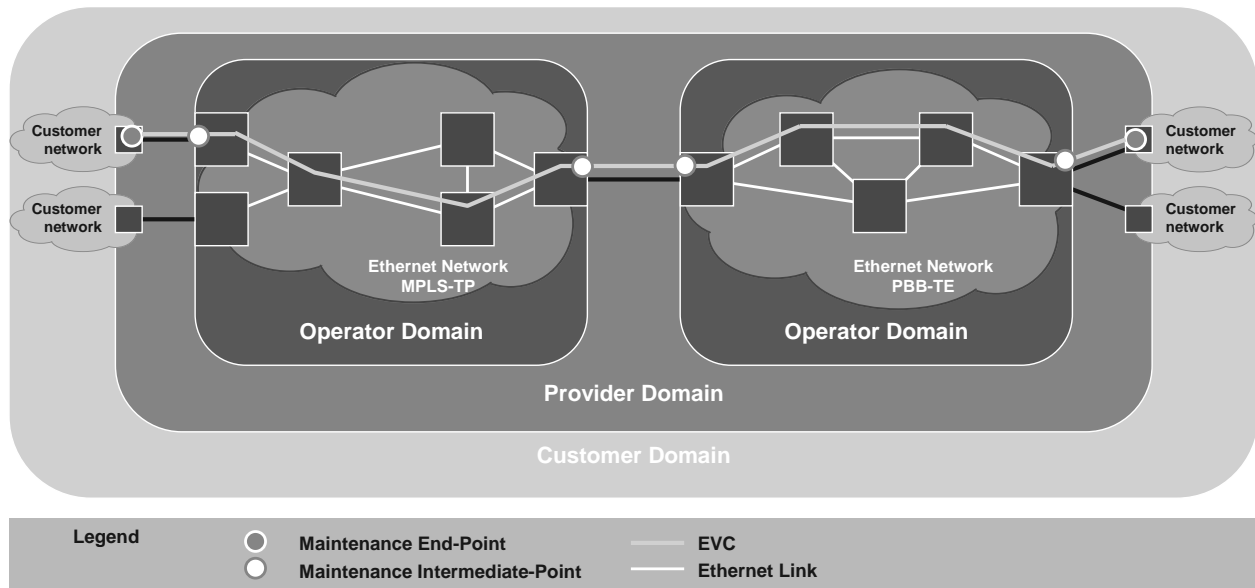


Figure 8: Customer insight in multi-domain network

4.4 Service Level verification

The fourth scenario is closely related to the former scenario. Instead of using Ethernet OAM for fault verification or isolation on end-to-end services the OAM functions can be used to verify how well the EVC service is performing in relation to the Service Levels agreed with the NRENs.

Availability can be measured using the standard fault detection mechanism Continuity Check. For instance CC messages could be sent on a one frame per second interval.

Regular automated performance measurements like packet loss, delay and delay variation could give insight in the average loss, delay and jitter performance of the EVC.

Important is to note that although this scenario is focussed on comparing the quality of the actual delivered service to Service Level Agreements and therefore is especially interesting for the customers, this scenario does not have to be operated by the customer itself. This could be a service operated by the operators and/or providers and delivered to the customers by monthly reports or (near-)realtime online reporting for instance.

5. Conclusions

With the introduction of Ethernet in the NREN environment Ethernet layer OAM will become increasingly important in the management of these networks. Especially in the case of services spanning multiple NREN domains where the NREN boundaries are interconnected on the Ethernet level. In multi domain NREN situations where end-to-end Ethernet connections are delivered Ethernet OAM can serve as the common technology to deliver end-to-end insight in the service delivered by the combined networks. The measurements can be used to visualise the state of the network or could for instance be used for anomaly detection. By enabling Ethernet OAM on specific nodes in a multi-domain NREN environment customers can gain insight in the service that is delivered to them by the NRENs. Next to measuring performance parameters using Ethernet OAM the information needs to be visualised and analysed. Most of the information measured by Ethernet OAM can be visualised using network management tools that are available at this moment. When Ethernet OAM is used in a multi NREN environment it is of great importance NRENs should negotiate what Ethernet OAM standards to support and what parameters to use.

As far as a single NREN domain is concerned, the OAM functions can be best executed by the transport technology most widely deployed within each domain. For instance, for networks using Ethernet transport technologies like PBB-TE, Ethernet OAM mechanisms are mandatory for the transport technology to work. However, for other networks with a large dominant IP/MPLS core, MPLS OAM mechanisms could prove more beneficial. With regard to MPLS-TP, the standards work is in progress and a choice has to be made between ITU-T Y.1731 based or a BFD based OAM mechanism. The current discussions in the IETF seem to lead to a combination of ITU-T Y.1731 and BFD based OAM mechanisms for the monitoring of an MPLS-TP network.

Acknowledgements

The authors are grateful to the Gigaport and GN3 projects for supporting the work presented in this paper.

References

- [1] Automated GOLE Pilot project flyer, <http://sc10.delaat.net/GLIFAutomatedGOLEPilot.SC.pdf>, 2010
- [2] Gigaport Project, <http://www.surfnet.nl/nl/Innovatieprogramma's/gigaport3/Pages/Default.aspx>
- [3] Géant GN3 project, http://www.geant.net/About_GEANT/Activities/Pages/ResearchActivities.aspx
- [4] Robert M. Metcalfe et al, Original Ethernet patent, <http://www.google.com/patents?vid=4063220>, 31 March 1975
- [5] IEEE Std 802.3ah, “Amendment to IEEE Std 802.3 – 2002: Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications”, 2004
- [6] IEEE Std 802.1ag, “Local and Metropolitan Area Networks, Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management”, 2007
- [7] ITU-T Recommendation Y.1731, “OAM functions and mechanisms for Ethernet based networks”, 2008
- [8] MEF 16, “Ethernet Local Management Interface”, 2006
- [9] ITU-T Recommendation G.8031, “Ethernet linear protection switching”, 2006

Biographies

Mark Prins holds a B Eng degree (*Cum Laude*, 2002) in Telematics and Computer Science from the Rijswijk University of Professional Technical Education. In 2002 he joined the Research & Development department of the ICT division of the Netherlands Ministry of Defence. After 3 years of research in the area of data communication over satellite networks in 2005 he joined The Dutch Organization for Applied Scientific Research (TNO) to become a scientist in the area of Future Internet. In this function he participates in several research projects on IP and Ethernet network architectures. He was involved in several European research projects including FP6 MUSE and Celtic RUBENS.

Richa Malhotra holds a BSc degree (*Honors*, 1997) in Mathematics from the Indian Institute of Technology, Kharagpur, India, a MSc degree (*Distinction*, 1999) in Applied Mathematics and a PhD degree (2008) in Computer Science both from the University of Twente, the Netherlands. From 1999 till 2009 she was a Member of Technical Staff at Bell Labs, Lucent Technologies and later Alcatel-Lucent, where she performed research on network protocols and algorithms for both wired and wireless networks. It was while working there that she also defended her PhD thesis. Since May 2009 she is working as a network architect at SURFnet. She is involved in the Next Generation Ethernet service design and architectural activities for SURFnet7 as part of the Gigaport3 project. She also co-ordinates the research activities carried out in collaboration with SURFnet’s research partners on various aspects of network modeling, design and performance.