Automated provisioning of Ethernet OAM in Carrier Ethernet networks: the case of GRNET

Leonidas Poulopoulos
(leopoul@noc.grnet.gr)
Network Applications Developer

Michalis Mamalis
(mmamalis@noc.grnet.gr)
Network Engineer

Stauros Kroustouris
staurosk@noc.grnet.gr
Network Applications Developer

Greek Research & Technology Network (GRNET) NOC
56, Mesogeion Ave.
11527 Athens, Greece

Keywords: Ethernet Operation Administration and Maintenance, VPN, monitoring, network automation, VPN, monitoring, network automation

Abstract: Ethernet OAM (Operation, Administration, and Maintenance) describes the monitoring of Layer 2 network operation by network operators. OAM is a set of functions that enables detection of network faults and measurement of network performance, as well as distribution of fault-related information. In this paper we will present a novel network automation framework developed in-house by GRNET NOC that configures and monitors Ethernet OAM over GRNET's provisioned Layer 2 services.

Ethernet Operations, Administration, and Maintenance (OAM) has become an indispensable tool that provides Network Operators and network management software a way to monitor the Layer 2 services and service parameters being offered. Operating independent of the actual Ethernet transport and the control plane of the service, Ethernet OAM provides information about the data path over which the service is carried. In that sense actual fault detection is being carried out by periodically sending connectivity fault measurement (CFM) messages along an end-to-end path of an Ethernet network.

The layered approach, supported by Ethernet OAM, allows for a more complex design in which the details of the end-to-end service layer are not exposed to the lower Ethernet Virtual Circuit (EVC/L2VPN) service layer. On the other hand nodes participating in the L2VPN service layer act as indicators for the upper layer allowing for a more fine grained monitoring. In that way if a defect, eg a network function not working as expected, continues to occur over a configurable time, a device considers the recurring defect a failure and thus raises an alarm.

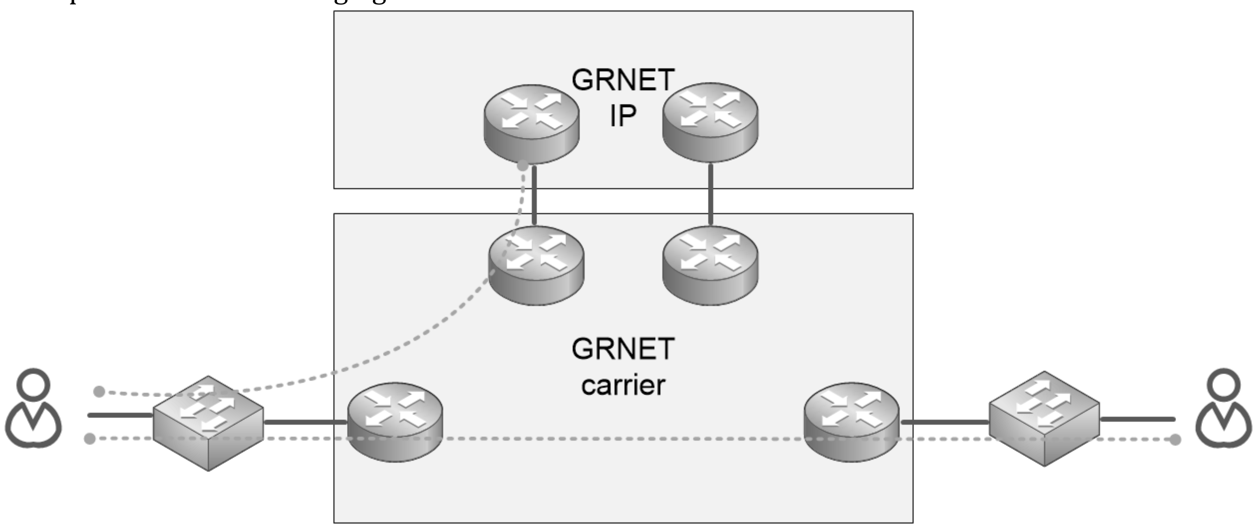
Implementation of Ethernet OAM, as defined by MEF 17 technical specification [1], comes in two flavors: IEEE 802.1ag [2] and ITU-T Y.1731 [3]. By merging the two standards together, the network is able of detecting faults along an end-to-end path of the Ethernet network while also providing performance measurements that monitor the following service attributes, Availability, Frame Delay, Frame Delay Variation ("Jitter") and Frame Loss both on the end-to-end service path and on the L2VPN carried within the MPLS network.

GRNET's network presents an ideal platform for the deployment of Ethernet OAM. The network architecture is a discrete 3-tiered design in which the access layer provides (only) Ethernet connectivity to Greek Universities and Academic institutions, the Backbone Carrier Network is a full

MPLS enabled cloud over which a number of L2VPNs carry customer traffic, while the IP layer is responsible for delivering IP connectivity and in doing so implements on of the end points of Ethernet OAM.

GRNET (Greek Research and Technology Network) provides Internet connectivity and services to the Greek Universities and academic and research institutes. GRNET maintains points-of-presence in all major Greek cities (approximately 40) and leases dark fiber across the country for its backbone and access network.

GRNET's network architecture allows for the provisioning of Layer 2 services (MPLS and Ethernet) as depicted in the following figure.



Layer 2 services are vastly deployed in order to provide IP connectivity to GRNET's clients along with point-to-point VPNs between them. However, we soon realized that monitoring at the interface level using traditional monitoring techniques such as interface status monitoring via SNMP, eg. Nagios, Icinga, Cacti, etc, proved to be inadequate. Thus, driven by the need to provide verification, monitoring, troubleshooting and service assurance for our Layer 2 services we developed an open-source network automation framework that primarily allows for provisioning of Ethernet OAM across our carrier network. The framework detects in an automated manner all the existing and new L2 services (MPLS and Ethernet segments). This is assisted by a network topology discovery tool that has a near real-time view of the provisioned Layer 2 services. During bootstrapping, the framework generates a set of proposed CFM setups that can either be applied in an automated or in a managed manner. In the latter case, a web UI is used by the network administrators to select the desired setup which is then applied to the network via NETCONF [4]. The novelty of the platform, however, is the automated way of provisioning Ethernet OAM. The platform has knowledge of the network and its active Layer 2 services. The source of information stems from a path-finding algorithm based on LLDP combined with the network devices VLAN inventory and the MPLS VPN index. This allows for automatically applying Ethernet OAM configuration via NETCONF per service to all devices that the service transits or terminates. Upon OAM CFM configuration application, a component of the framework initiates monitoring of the services via NETCONF. The average time to obtain all OAM statistics per run from 35 devices that provision approximately 230 VPNs is in the order of 60 seconds using the Python Threading

module with 6 workers. The results can, then, be fed into corresponding rrd files or they can be stored in a database. To keep track of the existing configuration, the framework performs regular reconciliation on OAM and generates validity reports. The platform provides APIs for monitoring systems (Icinga, Nagios) or can act as a standalone monitoring tool.
The platform has been developed in Python, makes extensive usage of the Python NETCONF library (ncclient) [5] and will be released in public as an open source project by GRNET NOC.

References

[1] Metro Ethernet Forum, Technical Specification 17, http://www.metroethernetforum.org/Assets/Technical_Specifications/PDF/MEF17.pdf

[2] IEEE 802.1ag, Connectivity Fault Management, http://standards.ieee.org/findstds/standard/802.1ag-2007.html

[3] ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks, http://www.itu.int/rec/T-REC-Y.1731/en

[4] RFC6241, Network Configuration Protocol (NETCONF), https://tools.ietf.org/html/rfc6241

[5] NETCONF Python client, ncclient, https://github.com/leopoul/ncclient

Vitae

Leonidas Poulopoulos received his Diploma in Electrical and Computer Engineering from the University of Patras in 2005 and his M.Sc degree on Computer Science from the Department of Computer Engineering and Informatics (University of Patras) in 2010. Currently, he is with the development team of GRNET NOC. He designs and develops network management applications and web platforms and quite often, a mix of both. His job/interest/research profile can be found at: http://www.linkedin.com/in/leopoul
email: leopoul@noc.grnet.gr
phone: +30 210 7471096, +30 697 3845436

Michalis Mamalis received his Diploma in Electrical and Computer Engineering from the Democritus University of Thrace in 2002. His diploma thesis focused on the design and implementation of an MMIC board acting as the optical receiver part of an STM-4 optical link. His areas of interest include MPLS, routing protocols, IPv6 and policy based networking. Currently he is with the network administration and operations team of GRNET NOC.
Email: mmamalis@noc.grnet.gr

Stavros Kroustouris received his Diploma from the Department of Informatics, University of Pireus, Greece in 2014. Stavros is with the development team of GRNET NOC. He designs and develops network automation and monitoring applications and when not coding he is the guitarist of the Greek post-sludge band *Allochiria*.
Email: staurosk@noc.grnet.gr