Management of Inter-Domain Dynamic Lightpaths

Ronald van der Pol
SARA, Kruislaan 415, 1098 SJ Amsterdam, The Netherlands

keywords: hybrid networks, lightpaths, network monitoring, network management

Abstract

Lightpaths are in use by scientists all over the world for a couple of years now. Most of these lightpaths are setup manually by the Network Operation Centers (NOCs) of National Research and Education Networks (NRENs). Projects like Phosphorus [1] are investigating ways to setup these lightpaths either by end-users or by programs (typically via web services). This paper discusses what this means for the NOCs managing the hybrid networks that are being used by these inter-domain dynamic lightpaths.

1 Introduction

The introduction of dynamically setup lightpaths poses several new challenges for operational management. One of these challenges is to find a way to cope with the alarms generated during the setup of these lightpaths. During the provisioning phase alarms will be generated on the network nodes. This is explained further in the next session. In section 3 the issues of monitoring these dynamic lightpaths are discussed. A monitor system needs a way to discover and identify dynamic lightpaths, monitor the operational status of each lightpath as soon as it is set up by the end-user, it need to have inter-domain support, etc.

2 Alarms During Provisioning

Lightpaths through SDH-NG networks consist of a sequence of crossconnects on the nodes. The configuration of these crossconnects on the nodes causes alarms on the nodes. E.g., when the lightpath is not yet completely setup the nodes will generate *unequipped* alarms. Also, the end-nodes will generate *link down* alarms when the lightpath is not setup completely end-to-end yet.

When lightpaths are set up manually by the NOC, the reason for the alarms mentioned in the previous paragraph can be correlated to the provisioning work done by a NOC engineer. This will be different when lightpaths are configured without involvement by the NOC, especially when there are lots of changes by lightpaths being setup and teared down.

In SURFnet6 DRAC [5] will be used to give end-users the possibility to dynamically setup lightpaths. A lot of effort was put into DRAC to minimize the alarms generated during the provisioning phase. Ports are put *Out Of Service* and in loop when they are unused. *Unequipped* alarms will be ignored. After a lightpath has been provisioned, the ports are put *In Service* and the lightpath is ready for use. This will minimize the impact of alarms during the provisioning phase.

Another reason for alarms is when the topology of a lightpath network is changed dynamically by end-users using UCLP. In 2007 optical multicast [4] was succesfully demonstrated during various conferences, e.g. GLIF and SC07. In these demonstrations about half of dozen sites participated. They were interconnected by lightpaths. A site would send video over a lightpath. This lightpath signal was split several times so as to send the same video stream to several other sites. Moreover, part of the lightpaths would be configured dynamically with the help of UCLP. This involved changing the topology of the lightpaths so that the video streams would go to different sites. This action would generate *unequipped* alarms on all the nodes and *link down* alarms on the end ports. The *unequipped* alarms could be ignored, but the *link down* cannot be ignored, because they could also be an indication of a real outage. This if still an open question that needs an answer.

3 Monitoring Dynamic Lightpaths

Monitoring involves knowing the topology and status of lightpaths. When the users experience a problem with their dynamic lightpath(s), the NOCs need to know the exact configuration and topology of the lightpath. This means there has to be way for the end-user and NOC to identify a particular lightpath. The NOC needs to figure out the topology of the lightpath and what section of the path causes the problem. This is especially tricky in the case of lightpaths that span multiple domains.

Spotlight [3] is a monitoring system that is used for SURFnet6 and NetherLight. It reads all information about provisioned lightpaths and status of the lightpaths from the network with the help of the TL1 Toolkit [2]. No manual configuration is needed. This means that dynamically setup lightpaths show up on the monitoring webpages automatically. Work is going on to setup a perfSONAR [6] compatible measurement point to publish the lightpath status information via web services in order to support inter-domain lightpath monitoring.

PerfSONAR is a system for monitoring inter-domain lightpaths. It consists of measurement points that provide the status of links. This information is made available via web services. Every domain runs one or more measurement points for the status of the links in its domain.

Currently, there are several shortcomings. Configuring the measurement points is a manual process. This means it will not work for dynamic lightpaths. Moreover, a unique lightpath name must be used by all domains. It is still an open question how a unique global identifier can be chosen in the case of dynamically setup ligthpaths.

By the way, these lightpaths are different from TCP circuits in an IP network. With IP, the network routing is setup such that there will be different paths and redundancy. Monitoring the status one particular TCP stream is not necessary because the stream will take a different route in case of an outage. Most lightpaths are unprotected. An fiber cut in the path causes an outage of the lightpath. Therefore, monitoing the status of lightpaths is important.

Acknowledgements

This work is funded by the Research on Networks project of SURFnet and the GigaPort project of the Dutch government.

References

[1] http://ist-phosphorus.eu/.

[2] http://nrg.sara.nl/presentations/glif-prague.pdf.

[3] http://nrg.sara.nl/publications/e-challenges-v1.4.pdf.

[4] http://www.glif.is/meetings/2007/controlplane/mambretti-hpdm.pdf.

[5] http://www.nortel.com/drac.

[6] http://www.perfsonar.net/.

Author Biography

Ronald van der Pol has been working in the field of Education and Research Networks for more than ten years. His former employers include SURFnet and NLnet Labs. At SURFnet he specialized on IPv6 and is co-author of several RFCs. In recent years his focus is on optical networks. He holds masters degrees in both Physics and Computer Science.