# Management of Inter-Domain Dynamic Lightpaths

Ronald van der Pol
rvdp@sara.nl
Deliverable D1.2.2/2.1.4.ii

December 2007

## 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). However, projects like Phosphorus [1] have begun to investigate ways to setup these lightpaths either by end-users or by programs (typically via web services). Also, Nortel's Dynamic Resource Allocation Controlller (DRAC) will be introduced as a service on SURFnet6 in 2008 to enable end-users to setup lightpaths through the SURFnet6 network dynamically. This paper discusses what dynamically setup lightpaths mean for the operational procedures of the NREN NOCs, and in particular for the SURFnet6/NetherLight NOC.

# Contents



# List of Tables

# 1 Introduction

Dynamically setup lightpaths create several new challenges to the operational procedures of managing lightpaths. One of these challenges is to find a way to handle 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 section 2. In section 3 the issues of monitoring these dynamic lightpaths are discussed. A monitoring system needs a way to discover and identify dynamic lightpaths, monitor the operational status of each lightpath as soon as it is setup by the end-user, it needs to have inter-domain support, etc.

# 2 Minimizing alarms caused during provisioning

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

When lightpaths are setup 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.

## 2.1 DRAC

In SURFnet6, DRAC [7] will be used to give end-users the possibility to setup lightpaths dynamically. A lot of effort was put into DRAC to minimize the alarms generated during the provisioning phase. Table 1 gives an overview of what alarms are generated in the various steps of provisioning of a lightpath.

DRAC tries to minimize the generation of these alarms when it provisions a lightpath. This is done in a couple of ways. First of all, on all customer ports a 1-WAY crossconnect from the WAN side to itself is set for all unused ports. This makes sure that the port does not generate alarms. When a lightpath is provisioned, the port is put in *Out Of Service* (OOS) state. The 1-WAY crossconnect is removed and the crossconnects of the path are provisioned. This generates *Unequipped* alarms. These alarms will be ignored by the NOC. After all the crossconnects are in place, the two end ports of the lightpath are put *In Service* (IS). This is done in a synchronized way in order to minimize the chance of a LINK DOWN or RDI alarm.

The previous paragraph describes how DRAC minimizes alarms during provisioning of a lightpath. However, this is only possible in the case where DRAC has direct control of all the nodes in the path, especially the nodes of the two end-points. For inter-domain lightpaths is will be difficult to suppress the alarms in the same way. This is something that needs te be investigated. These problems are the same for lightpaths setup by UCLP, as is described in section 2.2.

| near end crossconnect | far end crossconnect | facility state | near end alarm status |
|---|---|---|---|
| no | no | IS | ETH Link Down<br>ETH Loss of Data Sync |
| yes | no | IS | WAN Link Down<br>ETH Loss of Data Sync<br>VC-4 Unequipped |
| yes | yes | IS | no alarms |
| no | no | OOS | no alarms |
| yes | no | OOS | VC-4 Remote Defect Indication |
| yes | yes | OOS | no alarms |

Table 1: Reasons for Alarms

## 2.2 UCLP

User Controlled LightPaths (UCLP) is typically used to create Optical Private Networks (OPNs) with building blocks like nodes and links. These nodes and links are web services and are made available by UCLP to the end-user. In 2007 optical multicast [6] was succesfully demonstrated during various conferences, e.g. GLIF and SC07. In these demonstrations about half a dozen sites participated. They were interconnected by lightpaths. A site sent video over a lightpath and the signal was split several times so as to send the same video stream to several other sites. As part of the demo, some of the lightpaths were configured dynamically with the help of UCLP. This involved changing the topology of the lightpaths so that the video streams went to different sites. This action generated *unequipped* alarms on all the nodes and *link down* alarms on the end ports. The *unequipped* alarms are not a big problem. These can be ignored, as is done when using DRAC. But the *link down* alarms cannot be ignored because they can also be an indication of a real outage. This is still an open question that needs an answer.

## 2.3 DRAGON

Dynamic Resource Allocation via GMPLS Optical Networks (DRAGON) is used on Internet2 to setup dynamic lightpaths. In the Netherlands, the University of Amsterdam participates in the DRAGON project. DRAGON uses GMPLS to setup lightpaths. The provisioning phase is done via RSVP packets, currently mainly by configuring VLANs on Ethernet switches. However, work has started to support lightpaths on SDH-NG equipment too. Provisioning lightpaths on SDH-NG equipment will generate alarms just like the DRAC and UCLP cases. Lightpaths on Ethernet switches will usually not generate alarms, because the interfaces stay up all the time and only VLANs are setup and removed. The DRAGON circuits that run through NetherLight are used as Ethernet VLAN circuits. Therefore, in NetherLight we usually do not get alarms from dynamic provisioning of DRAGON yet.

# 3 Monitoring Dynamic Lightpaths

An important aspect of network management is monitoring. The monitoring system needs to provide a clear picture of the status and topology of all the lightpaths. When a user experiences a problem with its dynamic lightpath, the NOC needs to know the exact configuration and topology of the lightpath. The NOC needs to figure out which nodes are in the path of the lightpath and which section of the path causes the problem. This is especially tricky in the case of lightpaths that span multiple domains.

The end-user and the NOCs need a unique identifier for each lightpath to which they can all refer to in case of problems. In the case of dynamic lightpaths, it seems reasonable to request that the reservation and provisioning systems like DRAC, UCLP and DRAGON provide this identifier. This can be returned to the end-user when the end-user requests a lightpath. However, this name must also be provided to the NOCs. Although most equipments has support for configuring a name for crossconnects, it cannot be assumed that all domains use the globally unique identifier for this. Some might prefer their own local naming conventions and keep a mapping between globally unique identifiers and locally configured identifiers. How to handle this in the case of dynamically setup lightpaths needs to be worked out.

It is important to note that lightpaths are different from TCP circuits in an IP network. With IP, the network routing is setup in such a way that there will be different paths and redundancy between the end nodes. 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, monitoring the status of lightpaths is important.

## 3.1 Spotlight

Spotlight [5] is a monitoring system that is used for SURFnet6 [3] and NetherLight [2]. The web server part is based on Apache Tomcat and Java Server Pages. The information is presented to the user in the form of web pages. Spotlight uses two sources to get its data from. One of them is a topology file of the network. This is based on the Network Description Language framework [10] of the University of Amsterdam. The other is a database with all current network configuration information. The information about provisioned lightpaths and status of the lightpaths is read from the network with the help of the TL1 Toolkit [4] and stored in this database. 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 [9] compatible measurement point to publish the lightpath status information via web services in order to support inter-domain lightpath monitoring.

## 3.2 PerfSONAR

PerfSONAR [9] 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.

# 4 Conclusions

There are a couple of issues that need to be resolved in order to be able to manage dynamically setup lightpaths well. A proper way of handling of alarms is the most important issue. One could choose to ignore *unequipped* alarms. These alarms are an indiction of a lightpath that is not completely configured. This happens during the provisioning phase. But it can also occur when a lightpath is not completely removed, e.g. somebody forgets to remove one or more crossconnects. But this is easily solved by running scripts that check for crossconnect leftovers.

*Link down* alarms are more difficult. These will be generated on end-ports when the lightpath is being provisioned. But *link down* alarms can also be an indication of a real outage. When there is a real fiber cut in the same domain, there will also be a *link down* alarm for a backbone link. That needs attention. When the fiber cut is in another domain, the end-port still gets the *link down* alarm, but there is no corresponding *link down* alarm for a backbone link. One could choose to ignore *link down* alarms on end-ports too and only act on *link down* errors for backbone links. An inter-domain end-to-end monitoring system should take care of signalling outages in other domains.

It also seems practical to have a globally unique identifier to which the end-users and the NOCs can refer to. For dynamically setup lightpaths the reservation and provisioning system (DRAC, UCLP, DRAGON) the system has to generate this name and provide it to the end-users and the NOCs. The best way to provide the name to the NOCs is something that needs to be worked out.

One final conclusion is that there is a real need for an inter-domain end-to-end monitoring system. This means continued effort should be put into perfSONAR and Spotlight.

# 5 Acknowledgements

The analysis of alarms in DRAC was done by Thinh Nguyen (NORTEL), Andree Toonk (BC-NET, previously SARA) and Bram Peeters (SURFnet).

# References

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

[2] http://noc.netherlight.net:8080/spotlight.

[3] http://noc.sara.nl/spotlight.

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

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

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

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

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

[9] A. Hanemann, J. W. Boote, E. L. Boyd, J. Durand, L. Kudarimoti, R. Lapacz, D. M. Swany, J. Zurawski, and S. Trocha. PerfSONAR: A Service Oriented Architecture for MultiDomain Network Monitoring. In *Proceedings of the Third International Conference on Service Oriented Computing*, December 2005.

[10] Jeroen van der Ham, Paola Grosso, Ronald van der Pol, Andree Toonk, and Cees de Laat. Using the network description language in optical networks. In *Tenth IFIP/IEEE Symposium on Integrated Network Management*, May 2007.