UNIVERSITY OF TWENTE.

Last-Mile Lightpath Services
on packet-switched shared infrastructure

Master Thesis

Master's programme in Telematics (MTE),
Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS),
Design and Analysis of Communication Systems (DACS),
University of Twente, The Netherlands.

Author: Rudolf Biesbroek

Committee:

Dr. ir. Pieter-Tjerk de Boer	Universiteit Twente
Prof. dr. ir. Boudewijn Haverkort	Universiteit Twente
Dr. ir. Richa Malhotra	SURFnet

January 2014

Abstract

Lightpath services offer a great incentive for data-intensive scientific research and are widely used within and across NREN networks. Extending dynamic lightpaths into the last-mile in a flexible manner with very low provisioning time is the holy grail to achieve, since this would truly serve the end-user. However, the uptake of dynamic lightpaths in last-mile networks is low and a generic solution does not exist.

This empirical study investigates the possibilities to extend lightpaths on existing last-mile infrastructure. An experimental setup is used to examine the transmission characteristics when lightpaths are provided over an existing packet-switched last-mile infrastructure, and the consequences for the routed traffic.

The results revealed that in the absence of other traffic, no significant difference between the physical dedicated lightpath and the packet-switched lightpath regarding transmission characteristics is observed. However, under congested conditions a best-effort packet-switched shared infrastructure cannot prevent lightpath traffic from gaining a large part of the resources, thereby suppressing existing background traffic or vice versa. The study also revealed that using strict priority scheduling with traffic policing enables lightpath traffic to experience network performance as if no other network traffic exists, while limiting interference with existing background traffic. It can be concluded that QoS enabled network devices are able to provide lightpath connectivity on last-mile packet-switched shared infrastructures. Moreover, to improve network utilization, a Network Resource Manager (NRM) could be used.

This study provides insight into the feasibility to provide lightpath connectivity into the last mile and serve as basis for future studies. Moreover, the findings may support the decision making process to implement dynamic lightpath services in last-mile networks on existing infrastructures.

Acknowledgement

This thesis concludes my Master study Telematics at the University of Twente. I conducted this research for SURFnet under supervision of dr.ir. Richa Malhotra. Dr.ir. Pieter-Tjerk de Boer and prof.dr.ir. Boudewijn Haverkort provided supervision on behalf of the Design and Analysis of Communication Systems (DACS) chair of the University of Twente. I like to thank all three of them for their interest, guidance, and taking place as members of the graduation committee.

Special thanks go to the ICTS department of the University of Twente; to Jan Markslag for providing me the equipment, infrastructure, and other necessities to build and work on the experimental setup. Im also grateful for all the help, support and ideas provided by Jeroen van Ingen and Roel Hoek.

I'm very grateful to my family, who always believed in me, and their unconditional support. Special gratitude goes to Maria for the many hours of support, advice and motivation during the process of this thesis.

Rudolf Biesbroek
Enschede, January 2014

Contents

Chapter 1

Introduction

Lightpath services offered by most National Research and Education Networks (NREN) today offer a great incentive for data-intensive scientific research. They facilitate the transport of large data streams and can provide virtual dedicated connections, hereby bypassing the regular Internet. In addition, lightpath services are highly suited for less data-intensive streams as well. In the context of this work, a lightpath is defined as a point-to-point connection providing guaranteed bandwidth, packet loss, and minimal latency and jitter.

There is enough attention for dynamic and on-demand lightpath services within and across NREN networks. However, it should be noted that NRENs do not usually operate, control or manage the last mile campus networks to reach the end-user. Instead, last-mile networks or campus networks are usually maintained and controlled by institutes and universities. As a result, dynamic and on-demand lightpath services do not involve connectivity up to the researchers' desktop. The uptake of both static and dynamic on-demand lightpaths in campus networks is low and a generic and scalable solution to extend lightpaths into the campus does not really exist.

Realizing dynamic lightpaths into the last-mile network is the holy grail to achieve. In order to exploit the maximum benefits provided by on-demand lightpath services, they should extend to a (shared) research lab, or even better, to the desktop of the end-user in a flexible manner with very low provisioning time. Making lightpaths end-user configurable would result into more accessible services, which truly promote and facilitate data-intensive scientific research across the globe. For the uptake of lightpaths on the last-mile, more attention is needed to form a flexible and common

solution for the last-mile network. This study aims to contribute to the uptake of lightpaths by investigating possibilities to extend lightpath connectivity on existing last-mile infrastructure.

1.1 Last-Mile Requirements

Techniques used by NREN networks to provide dynamic lightpaths are not always applicable and different requirements and possibilities are relevant for last-mile networks. Investment on a separated dedicated layer2 network for the provision of (dynamic) lightpaths in last-mile networks is too costly. Furthermore, existing core network devices are expensive and replacement is undesirable. Therefore, sharing existing infrastructure is not only desired but also necessary for the uptake of dynamic lightpaths. A possible application for lightpaths over a shared campus infrastructure is constrained by the availability of existing hardware for last-mile networks. This constraint restricts the technologies available to use for the last-mile and is determined by the supported protocols by the hardware [46].

The challenge for last-mile networks is how to extend lightpath connectivity through their existing packet-switched shared infrastructure, i.e., what transmission techniques and architectures are suited for this demand. To achieve this, a flexible and scalable solution should be pursued.

The use of existing infrastructure for lightpath connectivity implies sharing available resources with existing production traffic. As a result, last-mile network administrators must trade-off between the high demands of lightpath connectivity, and the survivability of existing production traffic. Granting considerable amounts of resources to lightpath traffic can result in degraded network services for existing production traffic. On the other hand, provisioning lightpath connectivity while insufficient resources are available is disastrous for the guaranteed conditions of the lightpath traffic. QoS technique enables to differentiate between traffic and is considered as a candidate approach to provide lightpath connectivity on last-mile networks. Therefore, QoS will be included in this study.

1.2 Related Work

Few studies have examined last-mile network performances. An earlier study on lightpath applications concluded that packet-switched lightpaths on last-mile networks can cause deterioration for other last-mile traffic [35]. It is expected that this is especially the case when lightpath traffic is served with a Strict Priority (SP) scheduling strategy.

In earlier studies on IP/MPLS end-to-end differentiated QoS techniques, the performance results of IP QoS and IP over MPLS QoS have been widely investigated [41, 19, 43, 13, 31]. In general, these studies conclude that the investigated QoS techniques are performing well in order to differentiate traffic and provide services accordingly. Lightpath connections do not only provide guaranteed bandwidth, but also minimal loss, and low latency and jitter. However, these metrics are not always considered for the studies mentioned above. Not considering these metrics might nullify the advantages provided by lightpath connectivity. Consequently, QoS is often not thoroughly evaluated to draw adequate conclusions on the performance of last-mile lightpath connections.

This thesis contributes by gaining better insight into the interference of lightpath traffic with other traffic in the last-mile, thereby considering all lightpath performance metrics.

1.3 Goal

The purpose of this study is to investigate the transmission characteristics of a lightpath service, when extended into the "last-mile" by using existing hardware to accommodate not only dynamic lightpaths, but also existing IP-traffic. By investigating the transmission characteristics, an attempt is made to gain insight whether it is feasible to provide lightpath services over a packet-switched shared infrastructure (i.e., gaining similar performance metrics as a dedicated lightpath connection) and what consequences this may have for normal production traffic. These findings may support the decision making process to implement dynamic lightpath services in last-mile networks on existing infrastructures.

1.4 Research Questions

To achieve the above stated goal, the following research questions are formulated:

1. What are the effects on the transmission characteristics (i.e., latency, jitter, packet loss, guaranteed bandwidth) of a lightpath using last-mile infrastructure transmission technologies?

2. Considering a shared infrastructure (i.e., routed traffic and dynamic lightpath using the same hardware), what consequences does this have for the lightpath, and what are the consequences for the routed traffic (i.e., latency, jitter, packet loss, guaranteed bandwidth)?

3. Are QoS techniques required to provide or improve lightpath connectivity (i.e., performance guarantees of a lightpath) in the last-mile network?

1.5 Approach

Before starting this research, a literature study [15] has been performed to investigate what (dynamic) lightpaths are, and which candidate techniques are available to extend these lightpaths into the last-mile network. The literature study led to a set of techniques to extend lightpath services into the last-mile. From this set, VLAN and MPLS techniques are selected for this empirical study.

The hardware used in this study is selected by the network department of the University of Twente. The network devices support a set of QoS features and the selected transmission techniques for this empirical study.

An experimental setup is used to perform a series of experiments in order to find an answer to the aforementioned research questions (section 1.4). First, the performance metrics of a lightpath connection with physically dedicated resources with and without intermediated last-mile network devices are determined and evaluated. Second, the need for QoS when providing lightpath connectivity on a packet-switched shared infrastructure is examined. Third, the feasibility of lightpath connectivity on packet-switched shared infrastructure by applying QoS is investigated. Finally, performance metrics of MPLS and VLAN transmissions are compared.

The experiments are evaluated by means of different metrics (i.e., throughput, latency, jitter, and packet loss) and are reported on in this thesis.

1.6 Structure of the Report

The rest of this thesis is structured as follows. In chapter 2 background information about (dynamic) lightpath services is given. Chapter 3 explains the experimental setup. This includes the considerations for the experimental setup, the experimental overview, traffic generation, and monitoring and measuring of the experiments. The results collected from the experiments are analyzed and evaluated in chapter 4. Finally, chapter 5 concludes this thesis with conclusions, discussions and future work.

Chapter 2

Background

This chapter provides background knowledge to gain a broader view on the usage of (dynamic) lightpaths. This chapter consists of three parts, namely: *Lightpath Usage*, *Management and Orchestration of Dynamic Lightpaths*, and *Lightpath Connectivity into the Last-Mile*. These three parts are also reported on in the literature study [15] performed prior to this work.

The section *Lightpath Usage* (section 2.1) presents background information about the way lightpaths are used. This section discusses the different lightpath users, the use cases and applications of lightpaths, and infrastructure architectures of (dynamic) lightpath applications.

The section *Management and Orchestration of Dynamic Lightpaths* (section 2.2) includes information on available systems to administer and orchestrate the setup and tear down of lightpaths. These systems have a key function regarding the realization of dynamic lightpaths.

The section *Lightpath Connectivity into the Last-Mile* (section 2.3) presents information about the use of lightpath connectivity and involved aspects when lightpath connectivity is established in last-mile networks. This section discusses possible techniques to traverse the last-mile network, and what QoS can offer to differentiate between transmissions and provide distinct services to lightpath connectivity.

Finally, the section *Concluding* (section 2.4) ends this chapter with concluding remarks about this chapter.

2.1 Lightpath Usage

The Global Lambda Integrated Facility (GLIF) [5] is an international consortium promoting lambda networking, making lambdas available for scientists and projects involving large amount of data for scientific research on a global scale. Furthermore, GLIF is bringing knowledge together from experts all over the world by sharing experience, best-practice and encouraging shared development, testing and implementing lambda network technologies.

Together with participating GLIF members, a network of lambdas is created by interconnecting these lambdas through a series of exchange points known as GOLEs (GLIF Open Lightpath Exchange). A GOLE comprises of equipment that terminates a lambda, and is able to perform lambda switching. Different lambdas can be interconnected, creating an end-to-end lightpath.

Lambdas are high capacity optical wavelengths, which are able to transmit large amounts of information. On top of these lambdas, a lightpath can be established. Such a lightpath is a virtual circuit providing an end-to-end communication channel using some or all available lambda capacity, or it could even use the capacity of multiple lambdas.

The GLIF Automated GOLE pilot is working towards an automated provisioning system where lightpaths from different organizations can be interconnected, creating an end-to-end virtual circuit or lightpath. It leverages on the NSI protocol to standardize global inter-domain provisioning. The NSI protocol aims for standardized global inter-domain provisioning of high performance network connections. By means of the NSI protocol the Ethernet-switching GOLEs can be reconfigured to establish a dedicated VLAN between two end-points and provision this VLAN with requested performance characteristics [30].

The remainder of this section is based on two GLIF documents [11, 14]. These two documents — according to GLIF — describe researcher's experience, vision, and expectations for end-to-end lightpath connectivity across GLIF infrastructure with a focus on future technical direction, that is, what are the challenges ahead to be solved. This section is subdivided into three different sub-topics. The sub-topic *Lightpath Users* (section 2.1.1) discusses the different type of users of (dynamic) lightpath connections. *Use Cases and Applications* (section 2.1.2) discusses how lightpaths are used and for what purposes. Finally, *Infrastructure Architecture* (section 2.1.3) discusses architectures of dynamic lightpath applications.

2.1.1 Lightpath Users

It is expected that lightpath networking is not going to be used by most researchers within the near future. More likely, lightpath services will be more relevant in an indirect way for researchers through applications and middleware making use of lightpath connectivity.

Based on technology and level of control functionalities, three types of users can be distinguished: *Small and Medium Science Users*, *Big Science Users*, and *Guinea Pig Users*. The vast majority of users fall under the category *Small and Medium Science Users*. Although they require high quality network connection with low latency and high throughput, they mainly rely on normal IP connectivity. Usage of Bandwidth on Demand lightpaths is most likely not on an individual level, but might for example be used as an aggregated service in the campus core for connectivity to cloud computing.

Big Science Users are in need of large amount of bandwidth, extending 10 Gigabit/s and beyond. These users often share interconnected storage and use grid computing on a large scale, and require often international dynamic lightpath connectivity. The high connectivity needs of Big Science Users gave rise to the demand of lambda networking and can be associated with *Big Data Science*.

Big data science applications such as cloud computing, science as a service (SaaS), commercial data providers, large distributed sensor networks, and campus out sourcing and offloading are too large for traditional IP networks and could potentially disrupt other traffic. Claiming a large portion of the available resources would overwhelm traditional IP networks. Therefore, the new science is in demand for big pipes, creating their own dedicated network by interconnecting GOLEs. Hence, dedicated lightpaths will remain critical for big data science.

Early communication networks were hierarchical network architectures. However, it is suggested that data movement and replication in communication networks are often partial hierarchical [11]. A full mesh of interconnected networks is not practical and costly. Building a network where dynamical allocation of network capacity can be established in an on-demand way would reflect the need for data distribution more realistically as projects come online and distribute massive data-sets.

The last types of users are *Guinea Pig Users*. These are advanced users, willing to experiment with novel network architectures and services. Guinea Pig Users require a special kind of support where high-level experts are involved. They may provide useful early stage feedback during the development of new services, for example during beta-testing. These users can be associated with network innovation and development.

2.1.2 Use Cases and Applications

Lightpath Network applications can be divided into two groups: *direct lightpath connectivity* from the end-user, and *underlying lightpath connectivity* where the actual lambda connections are hidden to the end-user. IP networks are not always able to accommodate the large bandwidth requirements for big flows and provide the needed quality at the same time. In this situation direct lightpath connectivity can be used as a good alternative to QoS on IP switched networks. Underlying lightpath connectivity — where the actual lightpath connection is hidden from the end-user — is often used as a traffic engineering tool by network engineers but could even be used by applications in order to improve their connectivity over less congested paths.

Direct- and underlying lightpaths are used for various applications. An example of *direct lightpath connectivity* is for the connectivity to a Tier-1 Internet eXchange Points (IXP). Tier-1 IXPs can improve throughput by reducing RTT [23] on long distances by using direct lightpaths to various IXPs. Other examples are Science as a Service (SaaS) [16], Big Data Applications, and Large Sensor Applications such as the proposed Squared Kilometer Array [44]. *Underlying lightpath connectivity* can very well be exploited with research and education CDN (Content Delivery Network) applications. Also the aggregation of High Speed Wireless Network Applications can benefit from underlying lightpath connectivity, for example by offloading 3G/4G traffic [42] without any awareness of the end-user. Other examples where both types of lightpaths can be deployed are energy reduction [50, 45], and international collaborative experimental testbeds [3, 4]. The technical details to deploy lightpaths for these applications are still under development.

2.1.3 Infrastructure Architectures

Different end-to-end architectures are possible in order to realize an on-demand lightpath service across multiple GOLEs and networks. Few campus networks are directly connected to GLIF facilities and only a few universities and research institutes are able to dynamically switch optical lightpaths through their network. More often, an end-to-end lightpath connection is established between two GOLEs, rather than between two campuses. In that case, the GOLEs are used as a sort of DeMilitarized Zone (DMZ) where researchers locate their devices. If campus networks are fortunate to have a direct optical lightpath interconnected to a GLIF facility, they are often completely separated from the campus IP network, and responsible for their own security and connectivity. Unfortunately, this is still a long way from a generic, flexible,

and scalable solution for campus networks.

Recently, good results have been achieved regarding the establishment of lightpaths between various Autonomous Systems and GOLEs. But, connecting across campuses all the way up to the researcher's desktop has a long way to go. However, recent developments on Science DeMilitarized Zone (Science-DMZs) and campus Software Defined Networking (SDN) provide promising results. Still, interconnection and interoperability of DMZs, SDN, or other solutions remain very challenging towards the foreseeable future [24, 8].

In some way, GOLEs can be compared with the IXPs interconnecting the global Internet. GOLEs are crucial for global interconnecting NREN networks. Moreover, many GOLEs provide different functionalities, not only interconnecting optical lightpaths, but may also acts as DMZ, hosting computation and storage facilities. Furthermore, GOLEs might also be a logical place to serve CDN nodes and to provide hand-offs for wireless and Science as a Service applications.

One way to interconnect researchers with the GLIF infrastructure is by using general best-effort IP traffic. Hence, no transmission guarantees are provided. Another way to interconnect through the last-mile network is by extending (dynamic) lightpaths. NRENs such as SURFnet are able to provide (dynamic) lightpaths, interconnecting institutes with for example the GLIF infrastructure, or to other institutes. These lightpaths provide guaranteed bandwidth, packet loss, and minimal latency and jitter. On their turn, institutes are able to map lightpaths to (MPLS) tunnels or VLANs, for instance by using inter-domain provisioning tools such as NSI and IDCP (Inter Domain Controller Protocol). These tunnels or VLANs can easily be used to differentiate lightpath traffic from other traffic to provide the desired QoS. By doing so, last-mile networks can provide guaranteed bandwidth, packet loss, and minimal latency and jitter up to the researcher's desktop, in essence extending a lightpath into the last-mile network.

Also SDN networks are getting increasing attention of a growing number of campuses, data-centers, and research institutes. SDN — mostly OpenFlow — allows for easy and quick configuration of dedicated flows through the campus network to the researcher's workstation. Some research is currently conducted to examine the use of OpenFlow in order to map lightpaths to MPLS tunnels or VLANs using VRF (Virtual Routing and Forwarding), thereby improving isolation of lightpath traffic from other traffic [36, 33].

To overcome issues with the bandwidth and campus connectivity limitations, the concept of DMZ could provide a solution. Within such a DMZ, researchers can upload their data to a server which is directly connected to the GLIF optical network. In this case, the DMZ can be seen as a termination point, hiding the campus infrastructure from the outside world [12].

Terminating end-to-end lightpaths into the cloud may be an answer to a growing demand of cloud computing power and cloud storage. Large datasets can be stored into, retrieved from, and be worked with, within the cloud. Most commercial cloud providers are accessed by normal IP connections. However, researchers may be in need for direct connections independent of layer3 services for better performances. Although not all cloud providers are able to accept lightpath connections, they are able to handle large amount of data flows. In that case, NRENs are likely to act as a proxy to perform traffic engineering and manage lightpath connections [25].

Slightly different from the aforementioned scenario is when both ends of the lightpath are situated outside of the users' network. This could be the case when a lightpath is established between a remote instrument and a cloud storage facility, for example a lightpath from CERN to an arbitrary cloud provider. Providing resource control to a third party by delegating the control and management plane is a real challenge in such a scenario.

In a multi-domain BoD (Bandwidth on Demand) service, multiple technologies can exist in an end-to-end lightpath service. The JRA3 project defines a stitching framework which enables domains to use their technology of choice [22]. SURFnet 7 is the latest state of the art network of the Dutch NREN SURFnet. The technology of choice for this network is a PBB-TE Carrier Ethernet variant [32] and enables SURFnet to provide lightpath services in a flexible manner.

2.2 Management and Orchestration of Dynamic Lightpaths

In the previous section, the type of lightpath usage is discussed. This section includes information on available systems to manage and orchestrate the setup and tear-down of lightpaths. These Network Resource Manager (NRM) systems have a key function regarding the realization of dynamic lightpaths. The content of this section is not directly related to the performed research, but is related to dynamic lightpath connectivity and is referred to in the discussion of this thesis.

There are many NRMs available today to configure on-demand lightpaths services within a single NREN domain such as OpenDRAC [7], OSCARS [10], AutoBAHN [1], OpenNSA, G-LAMBDA, DynamicKL, etc. Furthermore, efforts are underway to extend the dynamic, on-demand lightpath concept over multiple NREN boundaries such as with the Automated GOLE project [2] within the GLIF (Global Lambda Integrated Facility, [5]).

NRMs make it possible to provide Bandwidth on Demand (BoD) services. According to the pan-European research and education network GÉANT3, BoD is a service to dynamic provision resources across multiple (NREN) networks creating a dedicated virtual channel for transmissions, demanding guaranteed capacity and high security by means of isolation from other normal Internet traffic. The NRMs are able to reserve or provision the necessary resources at the network components to provide the BoD service. In turn, the BoD service enables end-users to dynamically and in real-time set-up a point-to-point connection between two remote locations, reducing the gap between end-user applications and provisioning systems within the core network. The required characteristics of the connection can be acquired by using a web-based user interface.

Different NRENs are currently developing their own BoD tool. Some of them are compatible between operators, but not all. To realize interoperability among different provisioning systems — which realize bandwidth on demand over multiple NREN networks — two different protocols are in use, i.e., Inter Domain Controller Protocol (IDCP)[26] and Network Service Interface (NSI) [39] developed by the OpenGridForum.

To date, many NRENs are able to provide lightpath connections dynamically and in real-time. Reservations can be made through a web-interface, putting the control by the end-user. However, usage of a lightpath typically involves a point-to-point connection between two remote locations. The reservation at the NREN only involves the network of the NREN and does not include the last-mile.

In order to reduce the gap between end-user and the bandwidth on demand provisioning systems of the NREN networks, the GÉANT3 project studied the possible solutions to overcome the last-mile issue. A set of five solutions is considered [28]: Lambda Station, Terapaths, Phoebus, Virtual Routing, and generalized Token-Based Networking. These five candidates are selected based on the needs of the GÉANT3 project. The focus for a last-mile solution is on: TCP/IP protocol stack enhancement, low layer circuit provisioning (mainly layer2), and high performance network processors at the edge.

2.3 Lightpath Connectivity into the Last-Mile

This section presents information on lightpath connectivity into the last-mile, and is subdivided into two sub-topics. The sub-topic *Traversing the Last-Mile* (section 2.3.1) discusses possible techniques that enable a lightpath to traverse the campus infrastructure all the way up to the researcher's desktop. The sub-topic *QoS* (section 2.3.2) provides information on available techniques to provide special treatment for specific data transmissions. This knowledge can be used to improve lightpath connectivity. QoS enables to differentiate lightpath transmissions from other traffic and provide premium service to lightpaths.

Currently, best-effort Internet connections are used for many applications. Data flows are sent over a shared infrastructure with no additional guarantees on the delivery of data packets. For some applications, such as remote surgery, best-effort Internet connections cannot fulfill the required transmission demands. To overcome this problem, dedicated lightpaths can be used to connect over long distances with guaranteed bandwidth, latency, and jitter. However, dedicated lightpaths may be inefficient and costly in use when applications have a time-varying character (i.e., data flows are transmitted only a fraction of time), due to their static properties. Dynamic lightpaths as opposed to their static counterpart enable end-users to establish connections on demand and for a certain time interval. By doing so, a point-to-point connection is established between two interfaces with guaranteed bandwidth, latency, and jitter. In essence, the end user controls the network resources.

Researchers and other users at the institutions connected to NRENs such as SURFnet have a choice between the use of either a static or an on-demand lightpath. A static lightpath is a permanent connection but may be inefficient and costly when used for only a fraction of time. As opposed to their static counterpart, dynamic lightpaths are a temporary connection and on-demand variant, although with the

same characteristics as a static lightpath. This enables end-users to reserve resources in the network infrastructure and establish a point-to-point connection between two remote interfaces in an on-demand and real time fashion. Note that despite its name, a dynamic lightpath does not necessarily use only optical links.

Dynamic lightpaths up to the researchers desktop is the Holy Grail to achieve. Much effort is devoted to dynamic connectivity within and between NRENs. But this does not involve connectivity up to the researchers' desktop. Last-mile networks or campus networks are usually maintained and controlled by institutes and universities. Unfortunately, a generic, scalable, and flexible solution to extend lightpaths into the campus does not exist. For the uptake of lightpaths on the last-mile, more attention is needed to realize a generic, scalable, and flexible solution for the last-mile network.

This section discusses the requirements to extend lightpaths into the last-mile network. First, traversing a lightpath connection through the last-mile campus infrastructure is considered. Second, a frequently demanded requirement for lightpath services is considered — especially on a shared infrastructure — namely QoS.

2.3.1 Traversing the Last-Mile - Candidate Technologies

Most existing last-mile infrastructures such as campus networks are based on either a complete layer2 Ethernet based network or a combination of layer2 and layer3, with layer2 Ethernet in the access and aggregation and layer3 in the core. For such networks the question arises as to how the connection-oriented, guaranteed performance lightpath services should be configured. With respect to a packet-switched approach, the available options are MPLS, a simple VLAN based approach, an Ethernet encapsulation method (Q-in-Q, PBB) or a combination of these. MPLS is a technology which has been largely positioned for use in core networks. Therefore, the question arises if it is a good candidate for last-mile networks and what the right balance between added complexity versus costs and performance would be. MPLS is a technology which is not widely available on devices suitable for the access and aggregation layer within campus networks. As a result MPLS is not well versed by campus network operators. Provider Backbone Bridging is also a method which is not well-known within enterprises, or in this case, within campus networks.

Tunneling

Depending on the interpretation, a lightpath could be a layer3 or layer2 connection with certain guarantees such as minimal bandwidth. Providing layer2 lightpath services on top of a layer3 network infrastructure involves some kind of tunneling technique. By encapsulating the user frame information with a tunneling protocol, the original layer2 data can be carried over a layer3 network. Techniques used to acquire such a construction include L2TP, GRE, MPLS, and PBT [38]. Traffic isolation may be desirable for lightpath traffic. This can also be accomplished by tunneling, where all the traffic that belongs to a tunnel is not able to bleed to other traffic or vice versa. Moreover, isolation can ease QoS management. All aggregated traffic belonging to a lightpath tunnel can more easily be treated different from other traffic (i.e., guaranteeing minimum bandwidth).

Over-Provisioning

An alternative technique for QoS is over-provisioning. For a network with predictable peak traffic it may very well be possible to estimate and over-provision the available resources. This technique is reasonable for most applications and could be less costly compared to QoS investments. However, this approach does not provide any guarantees. With some greedy protocols — such as TCP — over-provisioning cannot prevent flows from increasing their throughput until all available bandwidth is used and packets are dropped. This results in increased latency and packet drops for all network traffic. Despite these shortcomings, over-provisioning is sometimes used as a solution to extend lightpaths into the last-mile network [18].

2.3.2 QoS

When using a dedicated connection, lightpaths provide a point-to-point connectivity with guaranteed bandwidth, packet loss and minimal latency and jitter. However, when a packet-switched infrastructure is used instead of a dedicated connection, resources are shared among other transmissions, often based on a best-effort approach. As a result, the guarantees of a lightpath cannot be given anymore. In this case, QoS techniques are able to provide guarantees to a lightpath, even when traversing a packet-switched infrastructure.

Different techniques are available to provide QoS. Two main types can be distinguished; Intserv and DiffServ. The former is a fine grained flow-based mechanism [20] and operates together with RSVP [21]. The latter is coarse-grained and is a class based mechanism. This type of QoS for IP is described in [37]. Architecture for DiffServ is described in [17] and MPLS support of DiffServ is described in [34].

A schematic description of DiffServ is shown in Figure 2.1 and Figure 2.2. Figure 2.1 illustrates the process when a packet is arriving at the label edge router (LER). At this point, packets are inspected based on their Multi-Field label (e.g., port, destination, source). Depending on the Service Level Agreement (SLA), packets are marked and shaped accordingly.

Within the Differentiated Services (DS) domain, QoS is provided based on Per Hop Behavior (PHB). Packets are inspected by their Differential Service Code Point (DSCP) and throughout the DS domain treated accordingly (Figure 2.2). The DSCP IP field consists of six bits which are used to distinguish between 64 different priorities.

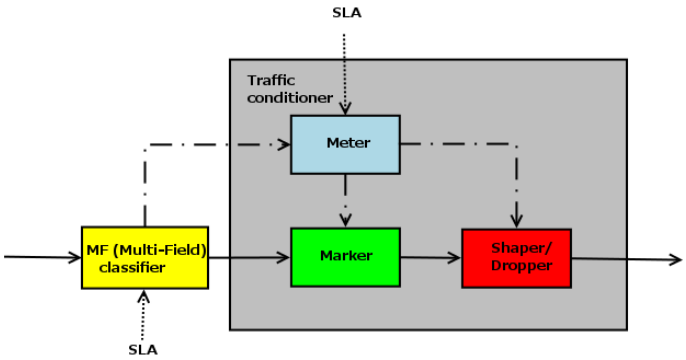


Figure 2.1. Packet Classifier and Traffic Conditioner.

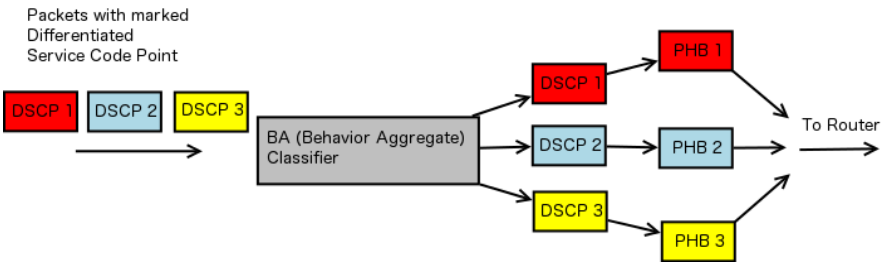


Figure 2.2. Behavior Aggregation Classifier.

Differentiating between different QoS levels can also be realized based on 802.1p bits and is part of the IEEE 802.1Q (VLAN tagging) standard. In order to provide lightpath-associated packets with a higher priority, the Priority Code Point (PCP) bits are set to differentiate from "normal" traffic. Alternatively, the MPLS EXP bits can be used. Both use a three bit field and therefore distinguish between eight different priorities. This approach makes it possible to provide QoS not only to IP-traffic, but other traffic as well.

Following below a description of bandwidth QoS configuration and queue scheduling is given. The former determines the available bandwidth and how bandwidth conformation is controlled. The latter considers queuing of incoming traffic and is an important configurable parameter, which strongly influences latency, jitter, and possible packet loss.

Bandwidth

Within a SLA different bandwidth profiles can be determined. A bandwidth profile is determined by the CIR (Committed Information Rate), CBS (Committed Burst Size), EIR (Excess Information Rate), and EBS (Excess Burst Size).

The CIR defines the average amount of traffic that is within the conformed bandwidth. Packets containing this traffic are denoted as 'green'. CIR-conform traffic is handled by the network according service performance objective. The CIR is an average rate because all frames are transmitted at line rate and not at for example the CIR itself. The CBS defines the maximum number of bytes allowed to receive at once, while still being marked as traffic within conformed bandwidth.

The EIR defines the average amount of traffic that is still accepted on the network, but is no longer within CIR-conform. The EIR is an average rate because all frames are transmitted at line rate, as already mentioned above. Packets containing traffic within the EIR are denoted 'yellow' and are being served as best-effort traffic and are eligible to packet discards. EIR-conform traffic is handled by the network but without any service performance objective. The EBS defines the maximum number of bytes allowed to receive at once, while still being accepted on the network as EIR-conform traffic. Packets containing traffic with an average rate greater than the EIR are denoted 'red' and are dropped.

Queuing Scheduling

An important feature of Ethernet devices is queuing. When a packet arrives at an Ethernet device, there is no guarantee that the device is able to process the packet right away. Therefore, an arriving packet is stored in a queue until the device is ready

to process the packet. First-In-First-Out (FIFO) is a very well known scheduling technique. All packets are treated in the same way and stored in a single queue. The order of arrival is also the order to serve the packets. This is a fairly simple scheduling strategy, but no service differentiation is possible. In order to take advantage of packets demanding lower quality of service, a FIFO queuing strategy is not sufficient.

By using different queues for different traffic priorities, QoS can be offered by differentiating between queues. More important traffic can be provided with lower queuing times compared to regular traffic. Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR) are known scheduling techniques to provide QoS [48, 29].

2.4 Concluding

This chapter provides background information on the topic of (dynamic) lightpath connections. Lightpath usage is discussed, lightpath users are identified, use cases and applications are described, and infrastructure architectures are specified. In line with this work, the goal to achieve is the extension of lightpath services into the last-mile network, using existing Ethernet switched infrastructure. By understanding the usage of lightpath connectivity, better knowledge on the needs to extended lightpaths is achieved.

The focus of extending lightpath connectivity into the last-mile will be on the *Small and Medium Science Users* and the *Guinea Pig User* and their use cases and applications. *Big Science Users* will most likely be in need for the physically dedicated lightpath connections and, therefore, fall outside the scope of this thesis.

Lightpaths can be deployed in various architectures, extending lightpath connectivity up the desktop is just one approach. This report considers an operational lightpath connection provided by an NREN up to the last-mile. By using a provisioning tool such as NSI, lightpath connections can be mapped onto VLANs or MPLS LSPs. Not considered in this report, but potentially promising techniques are SDN and VRF.

Management and orchestration of dynamic lightpaths is reported on in this chapter, but is not directly related to this research. However, understanding its role within NRENs provides better knowledge towards future work of dynamic lightpaths into the last-mile. It will have a key role in achieving scalable, flexible and on-demand established lightpaths into the last-mile network.

The last section of this chapter discusses candidate technologies and QoS matters related to extending lightpath connectivity into the last-mile. Today, NRENs are able to provide (dynamic) lightpaths to their costumers. To extend such lightpath connection, a set of candidate technologies is considered. From these technologies, VLAN and MPLS are selected for this study. VLAN technology is widely available within last-mile networks. MPLS is a technology largely positioned for core networks, but is getting more available for las-mile networks as well. MPLS is very suited for it's tunneling capacities, making it possible to traverse layer2 data through a layer3 network, in addition to traffic isolation.

Over-provisioning is sometimes used to extend lightpath services. However, no guarantees can be provided to the lightpath traffic, which potentially nullifies the advantages of a lightpath connection (i.e., guaranteed bandwidth, minimal loss, and low latency and jitter). Therefore, QoS is investigated to determine its added value. A DiffServ approach is considered to differentiate traffic on either VLAN or MPLS. In order to provide the best service available for lightpath traffic, a strict priority scheduling technique is chosen, providing lightpath traffic with the highest priority available. Besides providing priority to traffic, DiffServ also enables to control bandwidth allocation. By configuring a CIR value, a bandwidth restriction for the lightpath traffic bandwidth is realized. The effectiveness of this mechanism to lightpath and background traffic will be investigated.

Chapter 3

Experimental Setup

In this chapter the last-mile lightpath experimental setup design is discussed. The design is made with the network infrastructure of the University of Twente in mind. In this study a testbed is used to investigate the transmission characteristics of a (dynamic) lightpath in the last-mile, where existing hardware is used to accommodate not only (dynamic) lightpaths, but also existing routed IP-traffic. By investigating the transmission characteristics, an attempt is made to provide insight whether (dynamic) lightpaths provided by last-mile packet-switched shared infrastructures are feasible as an alternative for a physical dedicated connection.

The remainder of this chapter is organized as follows. First, in section 3.1, considerations for the design of the experimental setup are given. These considerations are important aspects in order to obtain a good abstraction of a real-world scenario. Second, in section 3.2, an overview of the experiment is given. This includes the testbed setup, and a description of the conducted experiments. Third, in section 3.3, the testplan used for this research is provided. Forth, in section 3.4, the approach for traffic generation is considered. Finally, in section 3.5, monitoring and measuring of the test results is explained, providing insight on the metrics used to evaluate the experimental setup.

3.1 Considerations

Most existing *last-mile* infrastructures such as campus networks are based on either a complete layer2 Ethernet based network or a combination of layer2 and layer3. For such packet-switched networks the question arises how a connection-oriented, guaranteed performance lightpath service should be configured.

In this study, both IP switched production data and lightpath traffic traverse the same hardware. However, the 'normal' IP traffic requires different network services compared to lightpath traffic. In most cases, a best-effort network service will suffice for normal IP traffic, while lightpath traffic demands for guaranteed bandwidth, packet loss, and minimal latency and jitter. Therefore, it is useful for the network to differentiate between traffic and serve according to transmission demands. Hence, traffic isolation and QoS are important and must be considered. For this reason, hardware and protocols should be able to comply with this.

When both lightpath traffic and 'normal' IP traffic are traversing the same hardware, some level of mutual interaction can exist. After all, they share the same infrastructure. If and how much this interaction is allowed, depends on the level of "Quality of Service". To some degree, interference with the 'normal' IP traffic is tolerable, since 'normal' IP traffic is served as best-effort traffic. However, large amounts of interference is undesirable and leads to bad performance and degradation of user experience for applications using 'normal' IP traffic. To what degree interference is still tolerable must be decided by the network administrator.

The testbed is designed keeping in mind a possible implementation into the existing campus infrastructure at the University of Twente. A good representation of the University Twente computer infrastructure (Figure 3.1) is a three-layer aggregation design, representing the core, a distribution layer, and a building distribution point. This infrastructure must be able to serve a (dynamic) lightpath connection providing a point-to-point connection between two remote hosts.

When a lightpath is established between remote hosts, it is assumed that traffic generated by a host is not exceeding the maximum bandwidth available for the lightpath. If the traffic generated is exceeding the maximum available bandwidth, packets must be dropped. Traffic policing may be used to control the amount of bandwidth gained by the lightpath (Figure 3.2). Dropping packets in order to stay conform bandwidth specifications should be done as close to the host as possible, preferable in the first hop, in order to prevent unnecessary data transmissions and thereby wasting available resources.

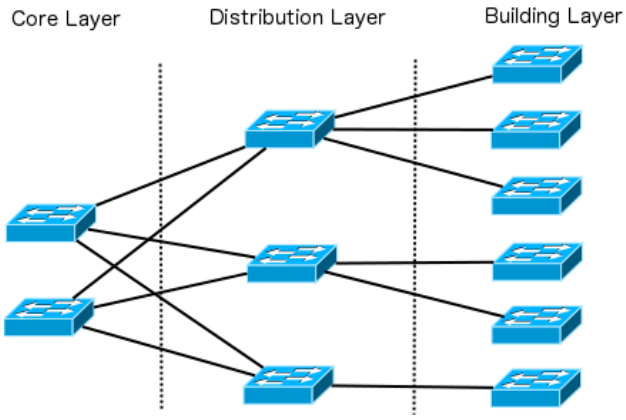


Figure 3.1. An abstract overview of the University of Twente campus infrastructure, representing a three-layer aggregation design.

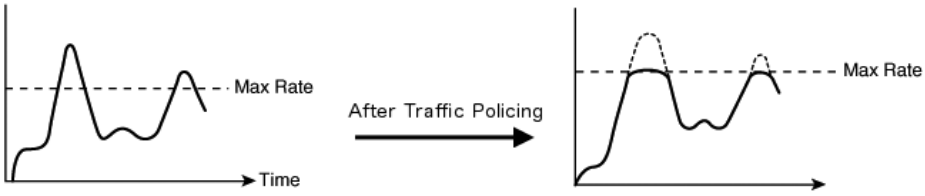


Figure 3.2. Traffic policing at work. Traffic exceeding the configured maximum rate is dropped. Traffic below the maximum rate is passed through as arrived.

To perform a useful investigation, the tests on the testbed are performed with various network loads and at least one test scenario must be performed where the aggregated bandwidth of both — IP switched production traffic and lightpath traffic — exceeds the available bandwidth for the next hop. By observing the system under overloaded conditions the performance of high priority traffic (lightpath) can be determined by comparing the results to the acquired guarantees.

3.2 Experimental Overview

In this section an overview is given of the testbed used for the performed experiments. The testbed setup reflects the three-layer aggregation design of the University of Twente campus infrastructure; representing the core, an aggregation layer, and a building distribution point. A set of experiments is designed and executed to determine the effects for lightpath and existing traffic when providing lightpath over a packet-switched shared infrastructure.

For the experimental setup, three HP A5800 switches are used and connected with 1Gbit Ethernet interfaces. Four ProLiant DL380 G4 servers with two Gigabit NICs, two 3.4 GHz processors and 4 GB internal memory, running Linux kernel version 3.5.0-17-generic are connected and used for the traffic generation and result analysis.

3.2.1 Tunneling

Traversing a layer3 infrastructure while providing layer2 lightpath connectivity is subjected to tunneling techniques. The switches used for this testbed are supplied with MPLS capabilities. By using this capability, layer2 packets can be encapsulated in an MPLS packet. Creating an MPLS tunnel through the layer3 core of the campus infrastructure enable layer2 lightpath services. By comparing the VLAN with the MPLS results, the performance of this encapsulation technique on the hardware under test is examined.

3.2.2 QoS

QoS is used to realize performance guarantees for the packet-switched scenarios of our experiment. Ethernet layer2 QoS is used to serve lightpath packets within the packet-switched network.

For the experimental setup, strict priority in combination with resource allocation is used. This enables the network to accommodate a lightpath on a packet-switched network, ensuring high priority (i.e., being served first) while limited in the attainable resources. Strict priority scheduling processes packets in the highest priority queue first. When the first queue is empty, the next queue is processed and so on, until new packets arrive at a queue with a higher priority. Hence, the lightpath experiences the network almost as if no other traffic exists. This ensures the best available service to the lightpath the network can offer. However, packet-switched network devices do not apply preemptive scheduling. Therefore, lightpath traffic can experience some effects of other traffic, when packets of lower priority are being served upon arrival.

In this study, two traffic streams are used; one stream represents the lightpath and the other represents the normal production traffic in campus networks. To prevent lightpath traffic exhausting available resources and starve production traffic, traffic policing is enforced at the ingress of the campus network (first access switch). This puts a limit on the maximum bandwidth which can be claimed by the lightpath. In addition, this value is easily configurable and manageable by the campus network operator.

3.2.3 Test Scenarios

The conducted experiments are divided into four different scenarios described below. Scenario 1 is used to determine reference measurements of the performance metrics of a lightpath when no other traffic exists. This scenario includes a dedicated lightpath connection to measure the performance metrics. A packet-switched share testbed configuration is used to determine the performance of a lightpath over a packet-switched infrastructure with intermediate packet-switched devices, but with all resources available for the lightpath connection.

Scenarios 2, 3 and 4 are all conducted on a packet-switched testbed and represents a situation where the background traffic and the lightpath traffic share the same packet-switched infrastructure. Scenario 2 is used to investigate the interaction between lightpath and other traffic, when lightpaths are provided on a best-effort packet switched shared infrastructure. Scenario 3 and 4 are used to examine a possible role for QoS to facilitate or improve lightpath connectivity over a packet-switched shared infrastructure.

By means of traffic generation and monitoring, results are analyzed and discussed. The techniques considered are: best-effort packet-switched, prioritized VLAN with resource allocation, and a MPLS LSP with resource allocation. Two different traffic flows are distinguished: a *lightpath traffic* flow, and all "regular" Internet traffic of the last-mile network, also denoted as *background traffic*. The background traffic is also represented as one flow for the sake of simplicity. By testing the system under different conditions the performance of the lightpath connection and the impact on the existing traffic is investigated. A testplan overview describing how the investigation is performed is described in section 3.3.

Scenario 1 – (*dedicated lightpath*). Dedicated and physical isolated last-mile lightpath. In this scenario the lightpath traffic cannot be interfered by background traffic. The lightpath traffic is operating over a point-to-point medium that is only used by the

lightpath itself; hence, not shared among others. This guarantees maximum QoS for the lightpath connection. Figure 3.3 depicts this scenario, showing the dedicated lightpath and the dedicated packet-switched lightpath containing intermediate switches. All measurements are taken between client and server.

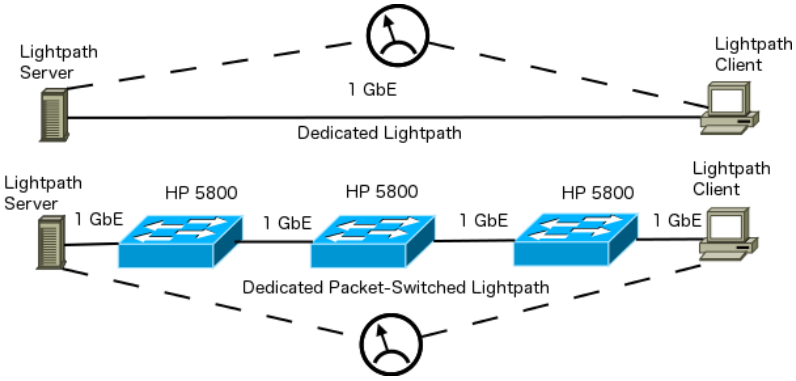


Figure 3.3. A schematic representation of the dedicated lightpath and the dedicated packet-switched lightpath testbed configurations used for the conducted experiments for scenario 1.

Scenario 2 – (*packet-switched lightpath*). A "traditional" best-effort-based IP configuration, where all hosts are placed in the same VLAN. In this scenario a shared infrastructure is used. Both lightpath and background traffic use the same infrastructure and compete for the available capacity. All traffic is sent based on a best-effort strategy, no QoS mechanism is used. All measurements are taken between client and server.

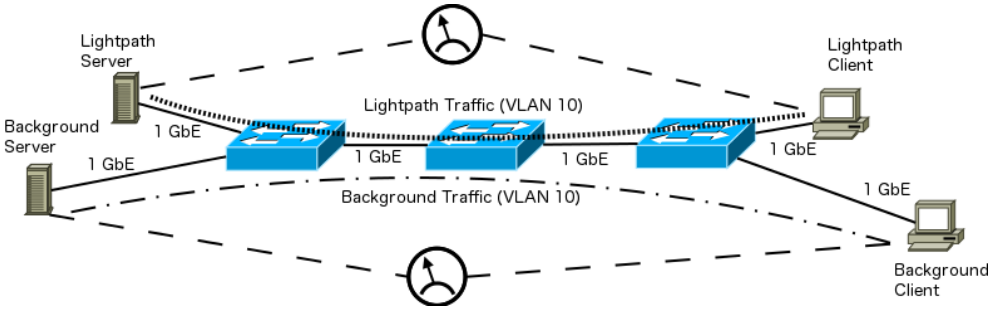


Figure 3.4. A schematic representation of the packet-switched testbed configuration used for the conducted experiments for scenario 2.

Scenario 3 – (*high priority packet-switched lightpath*). A VLAN-based high-priority packet-switched configuration where the lightpath receives priority over the background traffic. In this scenario production traffic is separated from the lightpath traffic by using two different VLAN-IDs, the lightpath traffic is served with higher priority by means of QoS techniques. All measurements are taken between client and server.

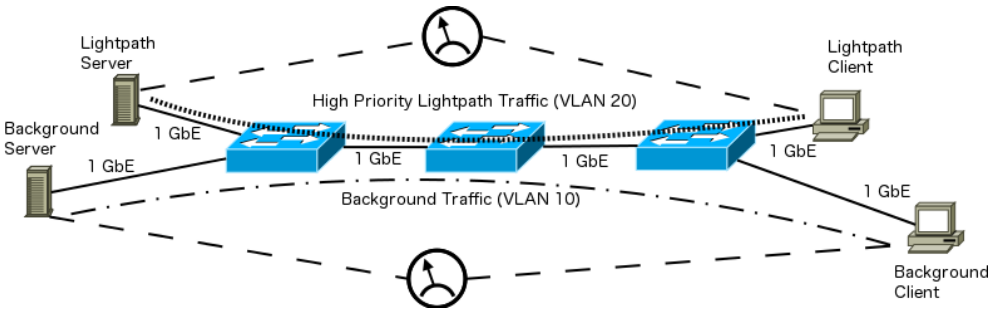


Figure 3.5. A schematic representation of the packet-switched testbed configuration used for the conducted experiments for scenario 3.

Scenario 4 – (*high priority packet-switched lightpath*). A MPLS-based high-priority packet-switched configuration where the lightpath receives priority over the background traffic. In this scenario production traffic is separated from the lightpath traffic. The production traffic is configured on a particular VLAN-ID, while the lightpath traffic is served by an MPLS tunnel connection and is served with higher priority by means of QoS techniques. This scenario reflects the desired tunneling capabilities for the last-mile infrastructure. All measurements are taken between client and server.

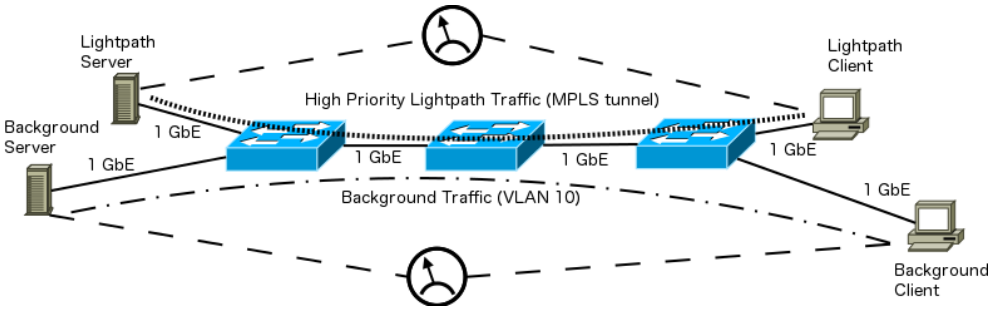


Figure 3.6. A schematic representation of the packet-switched testbed configuration used for the conducted experiments for scenario 4.

3.3 Testplan

This section provides an overview of the tests performed for this study. This overview shows how the different tests relate to each other, by discussing what tests are performed for which reason. The decision making process to determine which tests are needed for this work, also take into account the results of the previous executed tests.

Step 1 – Lightpath Comparison. To start, RQ 1 is considered. Therefore, a comparison is made between a lightpath connection using its own physically dedicated connection, and a lightpath connection over a dedicated packet switched infrastructure (no other traffic exists in this connection) as described for scenario 1. By comparing the results, an attempt is made to determine the effects on the transmission characteristics of a lightpath connection using last-mile infrastructure technology. TCP traffic is considered for throughput only (Table 3.1, test 1). Throughput, RTT, Jitter, Loss, Sent packets, and Received packets are considered for UDP traffic (Table 3.1, test 2–11). Instead of observing packet loss only, the amount of sent packets is considered too. The need for this raised during the execution of tests for scenario 1.

Step 2 – Lightpath and Background interference. Next we consider RQ 2. Based on the results of the previous step, only throughput is considered for TCP transmissions. Throughput, jitter, and RTT are considered for UDP traffic. For this step, test scenario 2 is used as described in section 3.2.3.

First throughput measurements are performed. A worst case test is performed where end-nodes transmit at maximum link capacity (i.e., 1 000 Mbits/s). A combination of TCP background and TCP lightpath traffic, UDP background and UDP lightpath traffic, and TCP background and UDP lightpath traffic are investigated (Table 3.2, test 1–3). Based on the outcome, the latter is compared to the results gathered at *step 3* to illustrate improved control when introducing QoS. A combination of UDP background and TCP lightpath traffic is left out of this investigation, because of the resemblance with Table 3.2 test 3.

To determine jitter and RTT behavior, UDP background and UDP lightpath traffic is investigated (Table 3.2, test 4). These results are compared with the results of *step 3*.

Step 3 – The Contribution of QoS. The third step considers RQ 3 where the contribution of QoS is considered in order to provide or improve lightpath connectivity into the last-mile infrastructure. For this step, scenario 3 is used as described in section 3.2.3.

As mentioned above, the throughput results of the combination TCP background and UDP lightpath (Table 3.3, test 1) are compared with the results of the previous step (Table 3.2, test 3). Also jitter and RTT results for combination UDP background and UDP lightpath traffic are compared (Table 3.3, test 2 and Table 3.2, test 4). To provide background and lightpath traffic with an equal share of the available resources, a CIR value is configured at 500 Mbits/s. This comparison provides insight into the improvement QoS is able to provide.

As mentioned in section 3.2.2, lightpath traffic (high priority traffic) could experience small effects on the existence of background traffic (lower priority traffic), even though strict priority scheduling is used. To investigate if TCP — as a connection oriented, congestion controlled protocol — may have different interference compared to UDP traffic, UDP lightpath performances are investigated, in combination with UDP, and in combination with TCP background traffic (Table 3.3, test 2–3). Based on the results, this experiment is not performed in the next step when MPLS is considered as a lightpath transmission protocol.

Step 4 – Compare Tunneling Approach. Finally, *step 4* considers MPLS as a tunneling solution. Here the VLAN results from test scenario 3 and the MPLS results from test scenario 4, as described in section 3.2.3, are compared. The lightpath transmission characteristics (RQ 1), the interference between lightpath and background traffic (RQ 2), and QoS are all considered (RQ 3).

First, the TCP lightpath throughput of scenario 3 and scenario 4 are compared, as well as their TCP background results. This comparison is performed by configuring the CIR value from 100 to 900 Mbits/s (Table 3.3, test 4–12 and Table 3.4, test 1–9). This represents different resource allocations for lightpath traffic.

Jitter and RTT are investigated in two different approaches: with and without congestion. The congested approach is used to investigate the worst case situation, where lightpath and background traffic are transmitting at line-speed (i.e., 1 000 Mbits/s). By configuring the CIR value from 100 to 900 Mbits/s, different lightpath resource allocations are represented (Table 3.3, test 13–21 and Table 3.4, test 10–18).

As mentioned in section 3.4.2, in a real-world situation, network administrators strive for little to none packet loss on their network. A more ideal situation would be when enough resources are available for both lightpath and background traffic.

Therefore, the aforementioned approach is also performed without congestion (Table 3.3, test 22–30 and Table 3.4, test 19–27). To accomplish this, lightpath traffic is configured 50 Mbits/s below the configured CIR value. The background traffic is configured with a transmission speed of 950 Mbits/s minus the CIR value. Resulting in a buffer of two times 50 Mbits/s. Below follows an overview of the different tests per scenario.

Test	Dedicated Lightpath		Switched Lightpath		Metric Set	Result Section
	Protocol	Mbits/s	Protocol	Mbits/s		
1	TCP	–	TCP	–	Throughput	4.1.1
2–11	UDP	100–1 000[1]	UDP	100–1 000[1]	T,L,R,J,Sp,Rp[2]	4.1.2

Table 3.1. Scenario 1 tests; Dedicated Lightpath

Test	Background		Lightpath		Metric Set	Result Section
	Protocol	Mbits/s	Protocol	Mbits/s		
1	TCP	–	TCP	–	Throughput	4.2.1
2	UDP	1 000	UDP	1 000	Throughput	4.2.2
3	TCP	–	UDP	1 000	Throughput	4.2.3
4	UDP	1 000	UDP	1 000	Jitter, RTT	4.3.1

Table 3.2. Scenario 2 tests; Best-effort

[1]The configured bit rate increases in steps of 100 Mbits/s for every next test
[2]Metric set: Throughput, Loss, RTT, Jitter, Sent packets, Received packets

Test	Background		Lightpath		CIR[3]	Metric Set	Result Section
	Protocol	Mbits/s	Protocol	Mbits/s			
1	TCP	–	UDP	1 000	500	Throughput	4.3.1
2	UDP	1 000	UDP	1 000	500	Jitter, RTT	4.3.1
3	TCP	–	UDP	1 000	500	Jitter, RTT	4.3.1
4–12	TCP	–	TCP	–	100–900[4]	Throughput	4.3.2
13–21	UDP	1 000	UDP	1 000	100–900[4]	Jitter, RTT	4.3.2
22–30	UDP	850–50[5]	UDP	50–850[1]	100–900[4]	Jitter, RTT	4.3.2

Table 3.3. Scenario 3 tests; High Priority VLAN

Test	Background		Lightpath		CIR[3]	Metric Set	Result Section
	Protocol	Mbits/s	Protocol	Mbits/s			
1–9	TCP	–	TCP	–	100–900[4]	Throughput	4.3.2
10–18	UDP	1 000	UDP	1 000	100–900[4]	Jitter, RTT	4.3.2
19–27	UDP	850–50[5]	UDP	50–850[1]	100–900[4]	Jitter, RTT	4.3.2

Table 3.4. Scenario 4 tests; High Priority MPLS

[3]CIR value in Mbits/s

[4]The configured CIR value increases in steps of 100 Mbits/s for every next test

[5]The configured bit rate decreases in steps of 100 Mbits/s for every next test

3.4 Traffic Generation

3.4.1 Background on Traffic Generation

Testing communication networks on their performance has been an important research topic for many years. One of the first models are developed by A.K. Erlang [27] in an attempt to qualify telephone switching networks. The current high complexity of Internet traffic, with its ever increasing number of applications, leads to a demand to generate and model network test traffic. However, despite many efforts of researchers, a general purpose traffic generator that is able to accurately mimic real computer network traffic does not exists yet. As a result, network applications can only be put under a specific test objective, which is an abstraction of a real-world scenario. Hence, the test objective determines the level of abstraction.

The purpose of network traffic generation falls into two parts [47]. The first purpose is to investigate on a particular network application, for example intrusion detection. Such a traffic generation tool may be very specific and quite possibly insufficient to investigate responsiveness, or even less suitable for other applications. Second, network traffic generation is used to produce background traffic. In this case, generated traffic is intended to represent desired network conditions for a particular network.

In both cases the generated traffic is used to represent an abstraction of a real-world situation. Analysis of the generated traffic can serve for the evaluation of real-world systems. This involves for example transmission performances of network applications like FTP clients or inter-arrival times of packets from VoIP applications. Unfortunately, due to limitations of network traffic generators, the investigated domain is not identical to the real-world domain, but always an approximation; both real-world traffic and generated traffic contain their own set of features. The intersection of these two sets are the features of the real-world that are actually put under test and determine the abstraction level of the investigated domain. Real-world features outside this set are ignored features, and features of the generated traffic outside the intersection are introduced by the traffic generator (illustrated in figure 3.7). Therefore, the level of abstraction for a given real-world scenario and the introduced feature set by the traffic generator must be taken into account when performing the investigation.

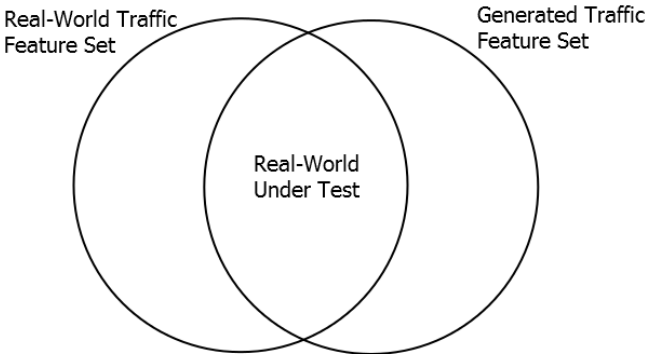


Figure 3.7. The two circles illustrate an abstraction of the real-world traffic feature set and the generated traffic feature set. The intersection contains the set of real-world features put under test; generated traffic is able to substitute real-world traffic for these features. Real-world traffic features not part of the intersect are ignored, while generated traffic features not part of the intersect are introduced, but do not exist in the real-world.

Network traffic generators are infeasible to generate completely realistic traffic. However, the majority of the popular network traffic generators target on one or more specific feature domains, such as: inter-arrival times, packet volumes, packet-length distribution, port distribution, bandwidth delay and latency, flows, load, think times, topology, and application content.

In general, three different types of traffic generators exist: *user-space traffic generators*, *kernel-level traffic generators*, and *hardware implemented traffic generators*. User-space traffic generators such as iperf [6] are popular for traffic generation. It is a common way to build traffic generator tools using the socket Application Programming Interface (API) of an operating system or a library providing low-level access to the Network Interface Card (NIC). For high speed and timely matters, user-space traffic generation tools are often not sufficient. Hardware implemented traffic generators are able to provide for maximum speed and precision, but lack usability, adaptability, and are very costly. Kernel-level traffic generators provide better speeds compared to user-space generators. Kernel-level traffic generators are closer to the hardware omitting additional user-space costs.

Alternatively, real-world data can be captured and replayed afterward using some kind of replay tool such as tcpreplay [9], and is a simple way to create application level content. However, this approach comes with some drawbacks. Captured data may contain sensitive information and to assure that privacy is guaranteed, captured information needs to be anonymized. Also, captured data contains behavior information of the monitored network at that time, but may not be representative when replayed in the testbed; all packets are regenerated in exactly the same way and no interaction occurs based on the current state of the network environment. This may be very suitable for specific application behavior, but less for the evaluation of other cases, for example TCP throughput measurements, due to its congestion control. Furthermore, the amount of useful data within a traffic capture might be low; only a fraction of the total captured data may be useful for the evaluation of network applications.

3.4.2 Concrete Setup

For the investigation of the experimental setup, network traffic is generated and sent on the testbed. As mentioned above (Section 3.4.1), two options are available to produce network traffic, either by replaying previous captured traffic, or by making use of a traffic generator.

In order to determine the effects of lightpath connectivity on packet-switched shared networks, it may seem obvious to use captured live network traffic and use this capture to replay on an experimental setup. However, this approach comes with some drawbacks as described above. For this investigation the content of the network traffic is of less importance. Rather the composition and amount of traffic is relevant.

When lightpath connection capabilities are implemented in a last-mile network infrastructure, a network resource management system should orchestrate the available resources. The amount of resources available for lightpath connections combined with the production traffic must not exceed the total available resources in order to avoid packet loss. In a real-world situation, the available resources for a lightpath can be determined based on historical network information. Furthermore, by using a buffer (i.e., allocating less resources for lightpath connectivity than maximum available), probability of packet loss is reduced even more.

Whatever technique is used to avoid packet loss, a real-world situation should strive for the least amount of packet loss and avoid exceeding the network's boundaries. Therefore, the performed experiments — where the boundaries are sought for — are stressing the network under test more compared to a real-world implementation. Hence, the network load of a real-world implementation is within — but certainly no more than the maximum achievable throughout of the experimental test setup. For this reason, results from the conducted experiments may yield a good representation of a real-world situation.

The performed experiments consist of congested and none congested tests. By controlling the amount of traffic and configuring resource limits as described in the concluding section 2.4 a buffer can be created to avoid packet loss, or congestion can be realized, depending on the needs of the test at hand.

The network performance is measured in terms of latency, jitter, packet loss, and throughput. These values are most significant at the boundaries; when the network load is high. A good approach in the context of this work is the usage of a network traffic generator. Iperf [6] is a simple cross-platform traffic generator tool. It is widely used for generating UDP and TCP traffic streams to perform throughput, packet loss and jitter measurements and is the network traffic generator chosen for the performed experiments. Latency measurements are performed by sending ICMP-packets with a `ping` tool. Hence, latency is measured as Round Trip Time (RTT).

The traffic pattern generated by iperf is a Constant Bit Rate (CBR). This is the only traffic pattern iperf is able to generate [40]. Obviously, this is an abstraction of real-world traffic, and it is expected that more realistic results are obtained if the chosen packet generator is capable to produce traffic with stochastical features for packet length and inter-arrival times. However, it is also expected that the introduction of more realistic traffic would not nullify the results of this study.

All tests are performed using a fixed time interval of 600 seconds. The dedicated lightpath test scenario is performed with only lightpath transmissions. All other scenarios are subjected to background and lightpath transmissions. During these scenarios the background traffic is sent during the total time interval. After 90 seconds, the lightpath starts sending for 390 seconds. When the test has been running for 480 seconds, the lightpath traffic stops, and only the background traffic continues.

3.5 Monitoring & Measuring

This empirical research on the performance of last-mile lightpath services is performed by transmitting and analyzing network traffic. In order to study and compare the different scenarios, a series of tests are conducted to measure the performance of the lightpaths.

Due to limitations of the used HP A5800 switch devices it is impossible to determine statistical information on interface level on the switch itself. Because of this limitation the measurements are performed on the application layer of the end-nodes. By performing the measurements on the application layer of the end-nodes, the results not only include network performances, but also the processing time of the end-nodes (Figure 3.8). Hence, the experiments reflect an end-to-end user experience.

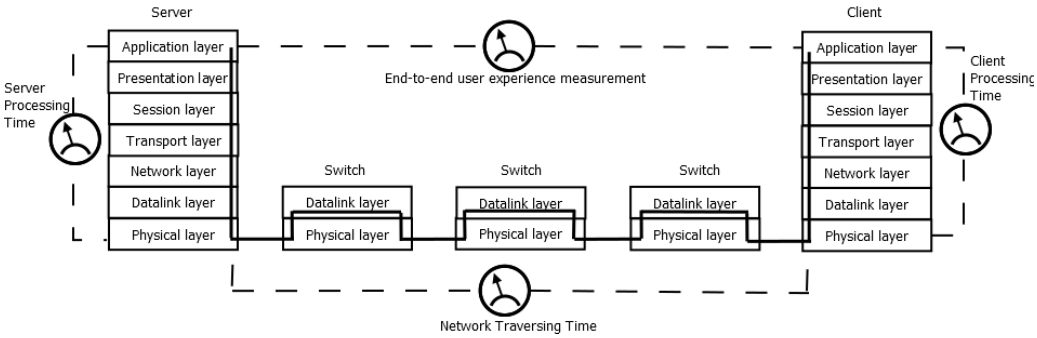


Figure 3.8. End-to-end measurement of the experimental setup. This includes client processing time, network traversing time, and server processing time.

In order to determine the performance of a lightpath, the throughput, latency (RTT), jitter, and packet loss are measured. Both TCP and UDP transmissions are considered in this study. One of the most important goals of TCP is to transmit data from source to destination as quick as possible and without any data loss. Therefore, the amount of throughput during a given time interval is an important performance metric and used to measure the TCP transmission performance.

UDP transmission is a connectionless transmission technique which does not guarantee the arrival of datagram information. It is often used for real-time applications where not only throughput and packet loss, but also latency and jitter are of importance. Therefore, with regard to UDP flows, the jitter (equation 3.1), RTT, and

packet loss are measured in addition to the throughput. All UDP transmissions are performed with a fixed payload size of 1 470 bytes.

Iperf is used to measure throughput, jitter, and packet loss, but does not give RTT values. Instead, ICMP packets are used to determine the RTT every second during the experiment. Values measured by iperf are also reported every second. RTT and jitter values for a given time interval or a complete run-time are expressed by calculated by the mean value of the reported RTT or jitter.

The jitter definition according to the iperf documentation is the smoothed mean of differences between consecutive transit times and is calculated as described in RFC 1889. The formula to estimate the jitter is:

$$J(i) = J(i-1) + \frac{|D(i-1,i)| - J(i-1)}{16} \tag{3.1}$$

where

$$D(i,j) = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i) \tag{3.2}$$

S_i is the transmission time-stamp of packet i and R_i the arrival time for packet i.

Chapter 4

Results

This chapter presents the results gathered from the experimental setup as described in the test scenarios in section 3.2.3. In section 4.1 the observed results of the dedicated (switched) lightpath are presented (Step 1, section 3.3). Section 4.2 presents the results of a lightpath connection served by best-effort techniques (Step 2, section 3.3). Section 4.3 presents the results when lightpath connections are served with high priority (Step 3 and 4, section 3.3).

4.1 Dedicated Lightpath

The results of the dedicated lightpath scenario are used as a reference for the other three test scenarios. Two different setups are compared; a physical dedicated point-to-point connection, and a dedicated packet-switched point-to-point connection where three switching devices are in between the end-nodes (section 3.2.3, Scenario 1). This section discusses the results of *Step 1 – Lightpath Comparison* as discussed in section 3.3.

4.1.1 TCP transmissions

The theoretical maximum throughput of a 1 000 Mbits/s Ethernet connection can be calculated as follows: a Gigabit Ethernet Interface is able to transmit 125 000 000 octets per second (see equation 4.1).

$$\frac{1\ 000 Mbits/s}{8bits} = 125\ 000\ 000 \quad octets/second \tag{4.1}$$

The maximum size needed to transmit one Gigabit Ethernet Frame, including MAC preamble (7 octets), Start Frame Delimiter (1 octet), Destination MAC Address (6 octets), Source MAC Address (6 octets), an optional 802.1Q VLAN-tag (4 octets), MAC Type or Length (2 octets), Payload(1 500 octets), Frame Check Sequence (4 octets), and Inter-Frame Gap (12 octets), is equal to 1 538 or 1 542 octets, without or with VLAN-tags respectively. The number of transmitted frames per second is with or without VLAN-tags respectively:

Without VLAN-tags:

$$\frac{125\ 000\ 000}{1\ 538} \approx 81\ 274 \quad frames/second \tag{4.2}$$

With VLAN-tags:

$$\frac{125\ 000\ 000}{1\ 542} \approx 81\ 063 \quad frames/second \tag{4.3}$$

For each frame a maximum of 1 500 octets are available for Payload. The experimental setup uses TCP/IP with timestamps (which requires 12 bytes), therefore, a total of 1 448 bytes is available for TCP payload data. This leads to a maximum TCP throughput of:

Without VLAN-tags:

$$1\ 448 * 81\ 274 * 8bits \approx 941 \quad Mbits/s \tag{4.4}$$

With VLAN-tags:

$$1\ 448 * 81\ 063 * 8bits \approx 939 \quad Mbits/s \tag{4.5}$$

Table 4.1 provides an overview of the measured throughput values of a dedicated lightpath and a dedicated switched lightpath. It shows that the dedicated lightpath is able to achieve a throughput of 941 Mbits/s. With a negligible difference of 2 Mbits/s caused by VLAN tagging of intermediate switches, the dedicated packet-switched lightpath achieves a throughput of 939 Mbits/s. These results are similar to the theoretical maximum throughput.

	Dedicated Lightpath	**Dedicated Packet-Switched Lightpath**
Throughput	941 Mbits/s	939 Mbits/s
Total transmitted	43 774 MBytes	43 661 MBytes

Table 4.1. *Scenario 1, test 1.* Dedicated Lightpath vs Dedicated Packet-Switched Lightpath. Average TCP throughput results during 390 seconds (t = 90-480)

4.1.2 UDP transmissions

The complete test comprises out of ten different configured throughput values in steps of 100 Mbits/s, ranging from 100 to 1 000 Mbits/s. For every configured throughput value, a total of ten test-runs are performed. From these test-runs, average metric values are determined. The minimum and maximum values are represented by the vertical bars.

RTT results

Figure 4.1 shows that the RTT values are slowly increasing with the throughput. Both the dedicated lightpath and the dedicated packet-switched lightpath show a large increase in RTT values at 1 000 Mbits/s. Although in general the RTT values of the packet switched-dedicated lightpath are low, compared to the dedicated lightpath they are structural higher.

Jitter results

Figure 4.2 shows the jitter values of the dedicated lightpath and the dedicated packet-switched lightpath. At lower throughput up to 100 Mbits/s, jitter values are approaching zero with values reaching as low as 1 μs and less. Jitter values are around 10 μs when the throughput is configured from 200 Mbits/s up to 800 Mbits/s. At 900 Mbits/s and 1 000 Mbits/s the interval of the minimum and maximum jitter values (vertical bars) are spreading out significantly. Although the dedicated packet-switched lightpath reveals higher values, with transmission speeds of 900 Mbits/s and 1 000 Mbits/s, the provided jitter values of both lightpath types are low on average. Overall, the trend of both lightpath types are alike.

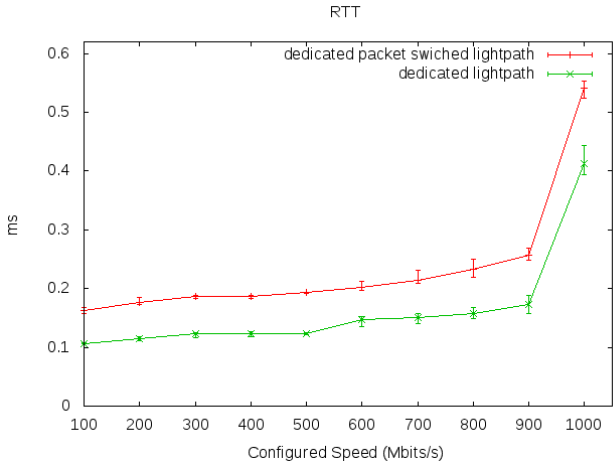


Figure 4.1. *Scenario 1, test 2–11.* RTT increases with increasing load.

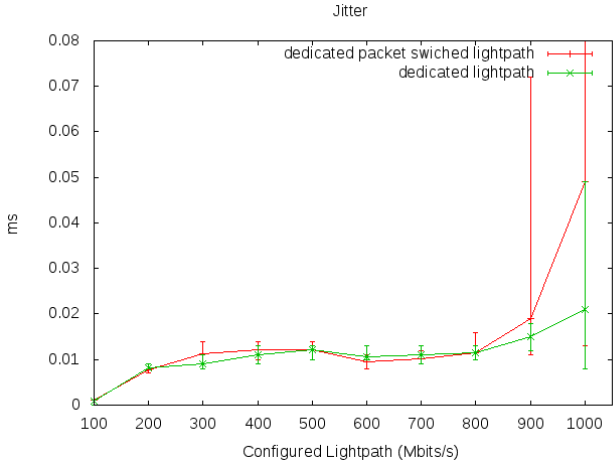


Figure 4.2. *Scenario 1, test 2–11.* Jitter increases with increasing load.

Packet loss results

Figure 4.3 shows the packet loss values of the dedicated lightpath and the dedicated packet-switched lightpath during the total run of the lightpath test. The observed packet loss is (close to) zero at lower throughput, but some losses do occur at lower

transmission speeds. With increasing throughput, a slow increasing trend of packet loss is observed. From 700 to 800 Mbits/s, a strong increase of packet loss is seen. At speeds of 800 Mbits/s and above, the growth in number of packet loss reduces. An unexpected decreasing trend is observed towards the maximum transmission speed of 1 000 Mbits/s. Packet loss reported by Iperf is also observed by the operating system. This means that the packet loss does not occur at the network, but rather at the Operating System (OS) level.

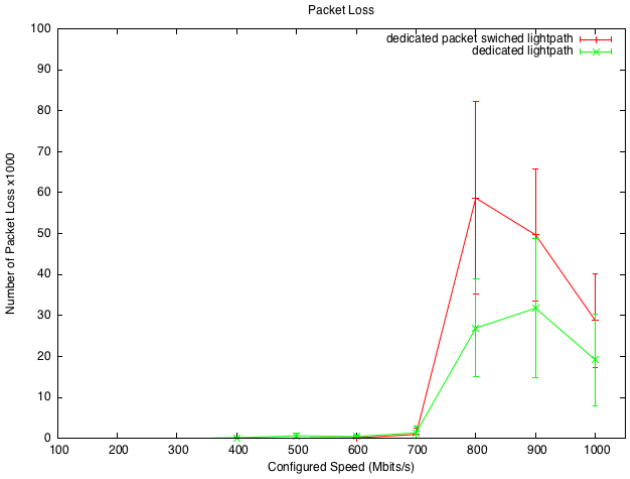


Figure 4.3. *Scenario 1, test 2–11.* Some packet loss is observed, especially when high speeds are configured.

Worth noting is that for the dedicated lightpath, a physically dedicated cable was used. Hence, no devices are placed in between the two end-hosts and no collisions are reported during the performed experiments. Although no packet loss should have occurred due to intermediate network components, Iperf did report packet loss. However, the reported packet loss by Iperf is equal to the number of packets discarded by the kernel of the receiving host. These packets are received by the kernel, but discarded because the kernel is unable to deliver the packets to the application. Hence, packets loss does not occur at the network, but rather at the Operating System (OS) level when passing information to the application. Therefore, it can be expected that the dedicated *packet-switched* lightpath is following the same trend.

Figure 4.4 shows the amount of Mbytes received during the performed test. Both lightpath types are showing the same trend. Up to a configured throughput of 700 Mbits/s, the amount of transmitted Mbytes increases, as expected, proportional to the configured throughput of Iperf. At 800 Mbits/s, the amount of transmitted information stabilizes; even though higher transmission rates are configured with Iperf, no increase of transmitted data is observed. Note that the amount of packet loss is very low compared to the amount of transmitted frames, and therefore cannot explain this behavior. The achieved throughput is not significantly influenced by packet loss, but rather by the amount of transmitted frames.

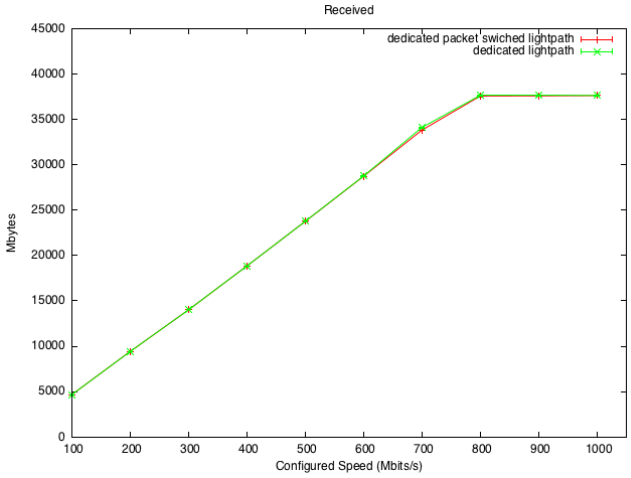


Figure 4.4. *Scenario 1, test 2–11.* Total received Mbytes is shown versus the configured transmission speed.

The number of transmitted frames is shown in figure 4.5. Up to 700 Mbits/s, a linear increase is observed in number of frames. This pattern is not surprising; when the transmission is increased, the number of frames (each with a fixed payload size of 1 470 bytes) should increase accordingly. From 700 Mbits/s this trend is slightly decreasing, and from 800 Mbits/s and higher, no significant increase of transmitted frames is observed.

Additional analysis have shown that this throughput problem is mainly caused by a deficiency at the source, somehow preventing the Iperf application from transmitting the required amount of packets. It was also found that this problem can be omitted by using two or more flows, after which Iperf is able to gain more throughput up to

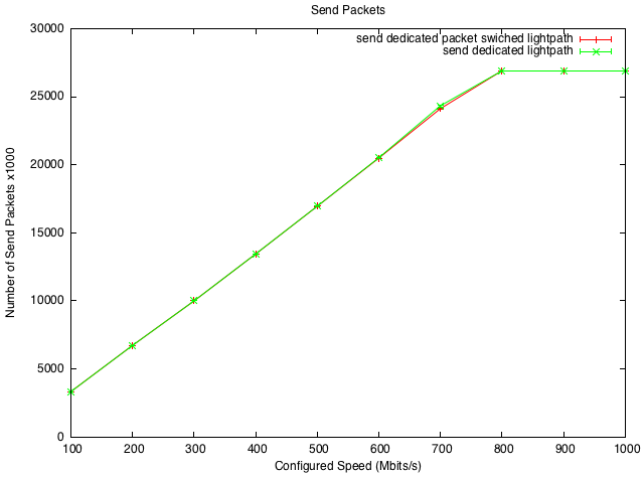


Figure 4.5. *Scenario 1, test 2–11.* The number of transmitted packets versus the configured transmission speed.

approximately 950 Mbits/s. Though, the exact reason for this deficiency of the source has not been determined and is subjected to future research. The observed behavior may indicate issues at the operating system level; apparently, the hardware is able to reach the desired throughput.

4.2 Best-effort

In this section lightpath connectivity is considered using "regular" best-effort transmission. Hence, no quality of service is provided. This section covers the results of *Step 2 – Lightpath and Background Interference* as discussed in section 3.3.

4.2.1 TCP transmissions

Table 4.2 shows the throughput results when both lightpath traffic and background traffic are TCP transmissions. Figure 4.6 shows the transmissions speed during an arbitrary test run. It can be seen in this figure that the background traffic is gaining close to 950 Mbits/s. As soon as the lightpath traffic starts, the background traffic and the lightpath traffic are competing for the available resources. The congestion control mechanism of TCP causes the background and lightpath traffic to share the available resources. The received amount of resources changes over time, but as expected, the information in table 4.2 shows that on average a fair share is gained.

	Background traffic	**Lightpath traffic**
Throughput	462 Mbits/s	477 Mbits/s
Total transmitted	21 484 MBytes	22 182 MBytes

Table 4.2. *Scenario 2, test 1.* Best-effort TCP background traffic and best-effort TCP lightpath traffic throughput results during 390 seconds (t = 90-480), showing negligible difference. Available resources are shared equally among the background and lightpath traffic.

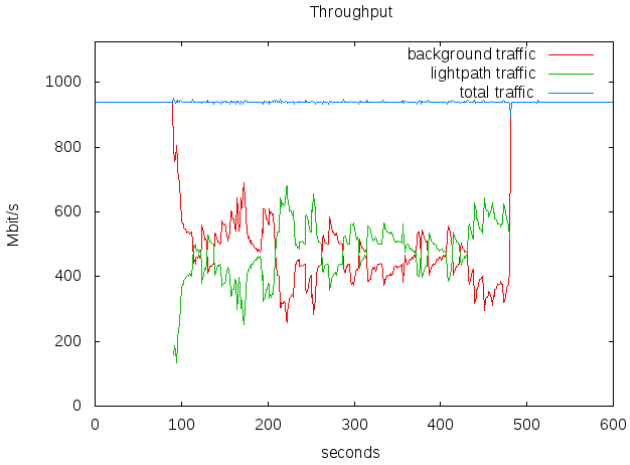


Figure 4.6. *Scenario 2, test 1.* Throughput in a best effort TCP transmission.

4.2.2 UDP transmissions

Table 4.3 shows the throughput results when both lightpath traffic and background traffic are UDP transmissions transmitting at 1 000 Mbits/s. Figure 4.7 shows the transmissions speed of a test run. It depicts how the background traffic is gaining close to 800 Mbits/s. As soon as the lightpath traffic is starting, the background traffic and the lightpath traffic are both gaining half of the resources. This behavior is expected, as both UDP traffic streams are transmitting at equal speed. As a result, an equal amount of traffic losses is observed during transmission. Eventually, the same amount of throughput is achieved. Table 4.3 shows for both background and lightpath traffic an average transmission speed of 477 Mbits/s.

	Background traffic	Lightpath traffic
Throughput	477 Mbits/s	477 Mbits/s
Total transmitted	22 193 MBytes	22 187 MBytes

Table 4.3. *Scenario 2, test 2.* Best-effort UDP background traffic and best-effort UDP lightpath traffic throughput results during 390 seconds (t = 90-480), showing equal distribution of available resources.

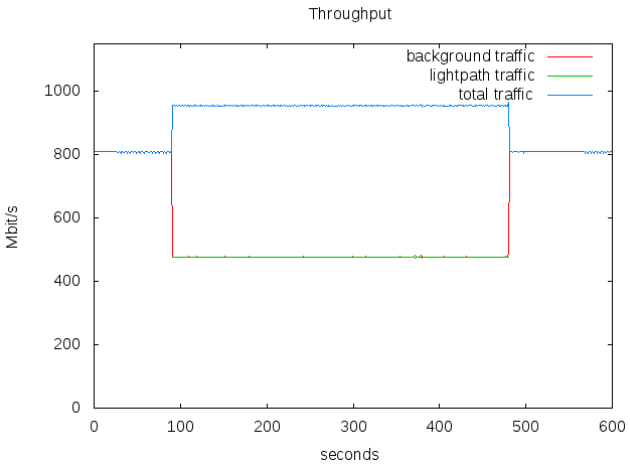


Figure 4.7. *Scenario 2, test 2.* Throughput in a best-effort UDP transmission situation. Lightpath and background traffic are gaining equal amount of bandwidth when transmitting together. Lightpath traffic is only transmitting during t = 90-480.

4.2.3 TCP – UDP transmissions

In the previous two tests the used transport techniques are the same for both the lightpath and the background traffic. In this test, a combination of TCP and UDP traffic is considered. Here, the lightpath traffic is configured as UDP traffic transmitting at 1 000 Mbits/s, while the background traffic is using TCP.

Figure 4.8 clearly shows how the lightpath traffic is able to gain large amounts of resources from existing background traffic. From Table 4.4 it is apparent that there is a large difference in achieved throughput in a time interval of 390 seconds.

	Background traffic	**Lightpath traffic**
Throughput	142 Mbits/s	810 Mbits/s
Total transmitted	6 609 MBytes	37 636 MBytes

Table 4.4. *Scenario 2, test 3.* Best-effort TCP background traffic and best-effort UDP lightpath traffic throughput results during 390 seconds (t = 90-480), showing the lightpath traffic gaining large amount of resources.

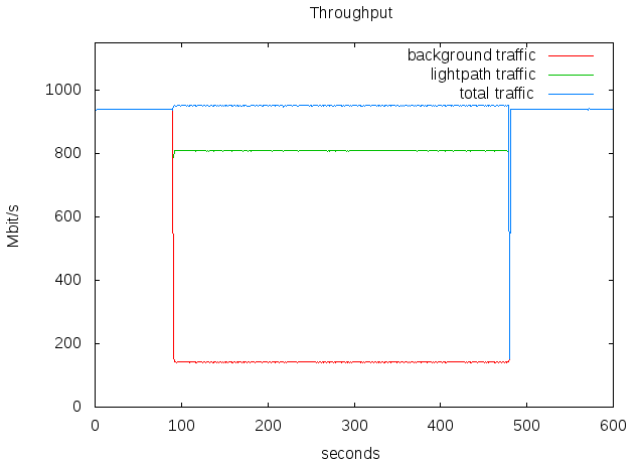


Figure 4.8. *Scenario 2, test 3.* Throughput in a best-effort TCP-UDP transmission situation. Lightpath traffic is only transmitting during t = 90-480.

UDP does not include a congestion control mechanism. Therefore, UDP does not react on the network conditions. The amount of obtained resources is determined by the transmission speed of the end-node and the number of packet drops. Therefore, an excessive number of UDP packets was able to gain large amount of resources, leaving

very little resources left for other traffic. High speed UDP transmissions may lead to excessive disproportional resource sharing.

The degree of impact that lightpath traffic is allowed to have on existing traffic depends on network policy and must be determined by the network administrator. This also holds vice versa, when background traffic is able to gain large amounts of resources, thereby putting heavy impact on lightpath traffic. Independent of the applied network policy, being able to control traffic behavior is not an unnecessary luxury.

Regardless of the selected transmission protocol, a best-effort network configuration does not include network control mechanisms. Consequently, it lacks the ability to support distinctive services for the allocation of resources and assigning different priorities to selected transmissions (e.g., lightpaths).

The next section discusses the results of the high priority packet-switched lightpath, in this scenario control on traffic behavior is enforced.

4.3 High-Priority Packet-Switched Lightpath

In the previous section a common best-effort technique is used to transmit background and lightpath traffic. Hence, the lightpath is served with equal service as the background traffic. In this section, the results are shown when the lightpath traffic is distinguished from the background traffic. The lightpath traffic is now served with higher priority and scheduled by strict priority strategy, preventing other traffic to interfere. The amount of reserved resources for the lightpath is determined by configuring a traffic policing profile. This prevents the lightpath traffic to starve other lower prioritized traffic.

Traffic policing enables high level of control on the amount of resources available to lightpath traffic. A CIR value configured on the network equipment puts a limit on the obtainable resources and prevents the lightpath from acquiring excessive resources, possibly leading to high impact on other traffic.

This section is divided into two parts. First, a VLAN configuration is considered in which the lightpath is assigned to a separate VLAN (section 4.3.1). Both source and destination are resided on this VLAN. Second, the results are presented when MPLS tunneling is used for the transmission (section 4.3.2), and how these results compare to a VLAN configuration.

4.3.1 VLAN

This section describes *Step 3 – the Contribution of QoS* as discussed in section 3.3.

Throughput

The results presented in this section are obtained by configuring TCP background traffic and UDP lightpath traffic, which both are transmitting at 1 000 Mbits/s. The lightpath transmission is restricted by traffic policing with a CIR value of 500 Mbits/s. However, the data in Table 4.5 shows that the lightpath is able to gain 486 Mbits/s of throughput.

This difference exists because of additional header information from the UDP and IP protocol. The used datagram size of the UDP packets during the experiment is set to 1 470 bytes. With a UDP header size of 8 bytes and an IPv4 header size of 20 bytes, the efficiency is 98,13 % (see equation 4.6). With a configured CIR value of 500 Mbits/s, the maximum achievable throughput is approximately 490 Mbits/s and is slightly higher than the actually achieved lightpath throughput of 486 Mbits/s.

	Background traffic	**Lightpath traffic**
Throughput	461 Mbits/s	486 Mbits/s
Total transmitted	21 458 MBytes	22 574 MBytes

Table 4.5. *Scenario 3, test 1.* VLAN strict priority packet-switched lightpath – TCP background traffic and UDP lightpath traffic throughput results during 390 seconds (t = 90-480). Lightpath is staying within configured CIR values and background traffic is gaining the remaining resources.

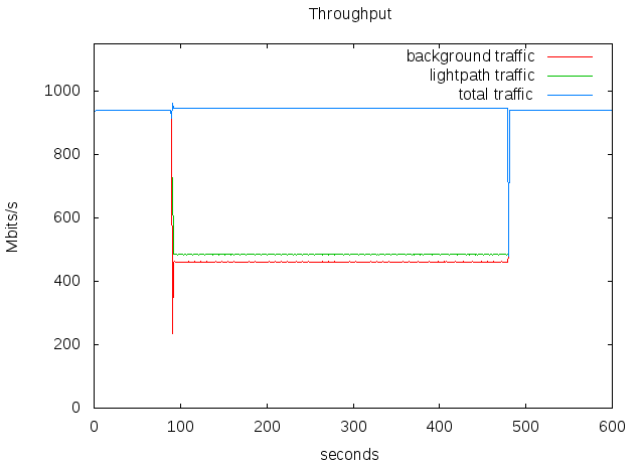


Figure 4.9. *Scenario 3, test 1.* VLAN strict priority packet-switched lightpath – Throughput overview of TCP background and UDP lightpath traffic. Lightpath traffic is only transmitting during t = 90-480.

$$\frac{1\ 470}{1\ 498} * 100\% = 98,13\% \tag{4.6}$$

In the previous test of TCP background traffic and UDP lightpath traffic (see section 4.2.3) — when all traffic is treated as best-effort traffic — resources are unequally distributed. The results for this test show that the lightpath traffic is not able to gain more resources than the configured CIR value of 500 Mbits/s, regardless

of any excessive data transmission. This allows other traffic to obtain a minimum amount of bandwidth (available resources minus CIR value), even though lightpath traffic is assigned with a higher priority and served with strict priority scheduling. Hence, the lightpath traffic is not able to starve other traffic.

Jitter and RTT - UDP background traffic

First, we consider jitter and RTT performance measurements for UDP background and lightpath traffic. The background traffic is sent during the complete run-time of the experiment, with a transmission speed of 1 000 Mbits/s. The lightpath traffic is also transmitted with a transmission speed of 1 000 Mbits/s, but only between 90 seconds and 480 seconds during the experiment. By concentrating on the jitter and the RTT values, a comparison is made between a best-effort configuration and a high priority lightpath configuration, with a CIR value of 500 Mbits/s (i.e., half of the available resources).

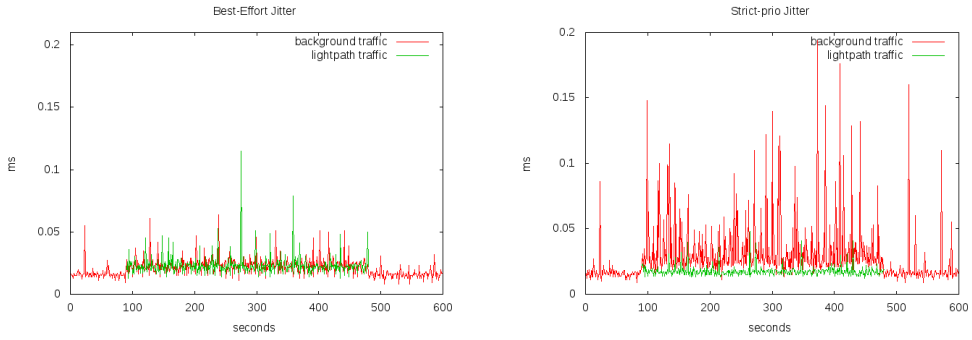
Table 4.6 provides an overview of the jitter values of the given experiments. During the first 90 seconds — when no lightpath traffic is transmitted — the jitter value for the background traffic shows negligible small difference between the best-effort configuration and the high priority configuration.

	Best-Effort		High Priority	
	t = 0-90	t = 90-480	t = 0-90	t = 90-480
background	0.016ms	0.023ms	0.017ms	0.035ms
lightpath	-	0.023ms	-	0.017ms
lightpath throughput		477 Mbits/s		485 Mbits/s
		(22 188 Mbytes)		(22 574 Mbytes)

Table 4.6. *Scenario 2, test 4 and Scenario 3, test 2.* Jitter results, best-effort vs high prio. Showing increased values for background traffic during transmission of lightpath traffic, while lightpath is receiving improved jitter values under high priority circumstances.

Lightpath traffic is transmitted between 90 seconds and 480 seconds. During this time interval, the best-effort configuration shows comparable jitter values for the background and the lightpath traffic (see figure 4.10a), both experiencing an average jitter of $0.023ms$ (see table 4.6). When the high priority configuration is used, a significant improvement for the lightpath traffic is observed. However, this comes with a drawback. Though still small, figure 4.10b shows higher and more varied jitter values for the background traffic. On average, the high priority background traffic is experiencing $0.035ms$ jitter. However, the increased jitter, compared to the best-effort configuration, is still small and acceptable for best-effort network applications.

The total throughput of the lightpath transmission is slightly different when comparing the best-effort configuration and the high priority configuration. The difference is due to the configured CIR value and enables the lightpath to gain slightly more resources as opposed to the best-effort configuration.



(a) best-effort jitter results

(b) high priority jitter results

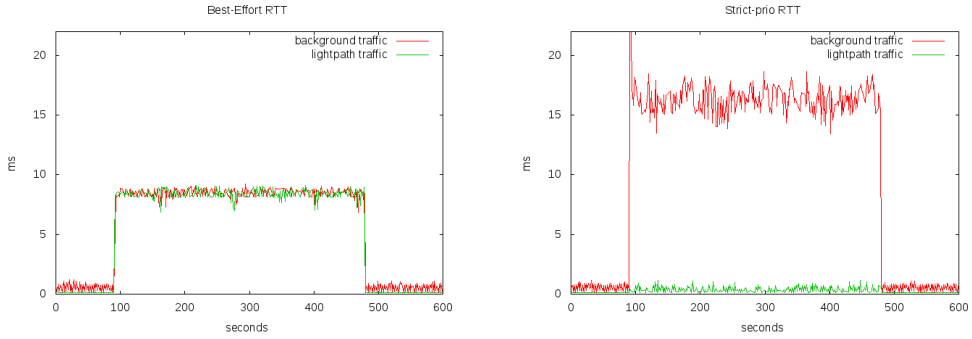
Figure 4.10. *Scenario 2, test 4 and Scenario 3, test 2.* Jitter results, Best-Effort vs High Prio. Figure 4.10a shows corresponding jitter values for both the lightpath and the background traffic. Figure 4.10b shows the background traffic is experiencing large variation in jitter. While the lightpath traffic is receiving improved jitter values compared to the best-effort configuration. Lightpath traffic is only transmitting during t = 90-480.

Table 4.7 provides an overview of the RTT values during the conducted experiments. During the first 90 seconds — when no lightpath traffic, but only background traffic is transmitted — the RTT value for the background traffic is on average equal in both configurations (i.e., best-effort and high priority). A small but negligible difference is observed for the lightpath traffic.

Between 90 seconds and 480 seconds, lightpath traffic is transmitted. During this time interval, the best-effort configuration is showing comparable RTT values for the background and the lightpath traffic (see figure 4.11a), experiencing an average RTT value of $8.48ms$ and $8.41ms$ respectively (see table 4.7). When the high priority configuration is used, a significant improvement for the lightpath traffic can be observed. However, this comes with an almost doubled RTT value of $16.29ms$. Even though, the reduced RTT is still small and acceptable for best-effort network applications. Figure 4.11b is illustrating the significant improved RTT value for the lightpath traffic and the almost doubled RTT value for the background traffic.

	Best-Effort		High Priority (CIR: 500 Mbits/s)	
	t = 0-90	t = 90-480	t = 0-90	t = 90-480
background	0.55ms	8.48ms	0.55ms	16.29ms
lightpath	0.15ms	8.41ms	0.14ms	0.41ms
lightpath throughput		477 Mbits/s		485 Mbits/s
		(22 188 Mbytes)		(22 574 Mbytes)

Table 4.7. *Scenario 2, test 4 and Scenario 3, test 2.* RTT results, Best-Effort vs High Prio showing increased values for background traffic during transmission of lightpath traffic, while lightpath is receiving improved RTT values under high priority circumstances.



(a) best-effort RTT results

(b) high priority RTT results

Figure 4.11. *Scenario 2, test 4 and Scenario 3, test 2.* RTT results, Best-Effort vs High Prio. Figure 4.11a shows corresponding RTT values for both the lightpath and the background traffic. Figure 4.11b shows that the background traffic experiences almost double RTT values, while the lightpath traffic receives significant improved RTT values compared to the best-effort configuration. Lightpath traffic is only transmitted during $t = 90$-480.

Jitter and RTT - TCP background traffic

Above, UDP background traffic is considered. UDP traffic is transmitted with a constant bit rate in a fixed interval. Consequently, the load on the network during lightpath transmission stays constant during the experiment. TCP on the other hand changes its window size over time, which determines the amount of information allowed to be sent without acknowledge message from the receiver. TCP is trying to set this window as large as possible to achieve maximum throughput. To avoid packet losses, the window size is decreased. This happens when the network gets congested (i.e., congestion control), or when the receiving host can not cope with the amount of information and needs to throttle down (i.e., flow control). As a side effect of this behavior, the transmission speed is not constant. To investigate the effects on jitter and RTT on lightpath traffic, TCP background traffic is now considered.

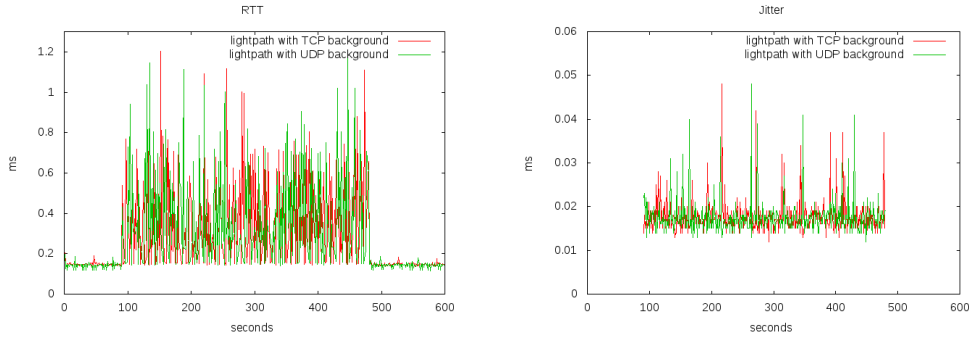
During the complete run-time of the experiment, TCP background traffic is transmitted. The lightpath traffic is transmitted with a transmission speed of 1 000 Mbits/s, but only between 90 seconds and 480 seconds during the experiment. The configured CIR value for the lightpath traffic is 500 Mbits/s.

Table 4.8 provides an overview of the average jitter and RTT values for the lightpath. The table compares the results when UDP or TCP background traffic is used. Figure 4.12a and Figure 4.12b show the RTT and jitter during the experiment, respectively.

In both figures (4.12a and 4.12b) no significant difference is observed. The lightpath transmission during TCP background shows the same performance trend on jitter and RTT as lightpath transmission during UDP background traffic. Also, when an average is calculated on al jitter and RTT values, a negligible difference is observed (Table 4.8). Independent of the used background traffic, lightpath transmission does not experience any difference in RTT and jitter.

	lightpath with UDP background	lightpath with TCP background
RTT	4.08ms	3.90ms
jitter	0.017ms	0.018ms

Table 4.8. *Scenario 3, test 3.* Lightpath RTT and jitter results – TCP vs UDP background traffic.



(a) lightpath RTT

(b) lightpath jitter

Figure 4.12. *Scenario 3, test 3.* Lightpath RTT and jitter results – TCP vs UDP background traffic. Lightpath traffic is only transmitting during t = 90-480.

4.3.2 VLAN vs MPLS

In this section a comparison is made between a VLAN and a MPLS configuration according to *Step 4 – Compare Tunneling Approach* as discussed in section 3.3. First, the TCP throughput is considered. Second, a worst-case scenario is presented where the background traffic and the lightpath traffic both transmit at 1 000 Mbits/s. In this scenario the RTT and jitter performance are observed. Finally, a more realistic real-world scenario is considered, where a buffer is kept between the available resources and the used resources for the background and lightpath traffic. In this case a CIR value is set; the lightpath traffic is configured to transmit at 50 Mbits/s below the configured CIR value, and the background traffic is configured at 950 Mbits/s minus the CIR value. This results in a buffer of two times 50 Mbits/s. All points in the figures are averages of ten measurements. The maximum and minimum observed values are depicted by the vertical lines.

Throughput

Figure 4.13 presents the achieved TCP throughput given the configured CIR value. The maximum lightpath throughput is controlled by the configured CIR value. The remaining resources are available for the background traffic. The lightpath traffic throughput performs alike, regardless of VLAN or MPLS configuration. The lightpath is able to gain the amount of resources set by the CIR. Remaining resources are available to the background traffic. When the background traffic and the lightpath traffic are accumulated, the VLAN configuration gains a total throughput of 939 Mbits/s, which is equal to the dedicated packet-switched lightpath throughput (see table 4.1). For the MPLS configuration, a small decrease is observed compared to the VLAN configuration, up to 12 Mbits/s when the CIR value is configured at 900 Mbits/s. This difference resides completely at the background traffic.

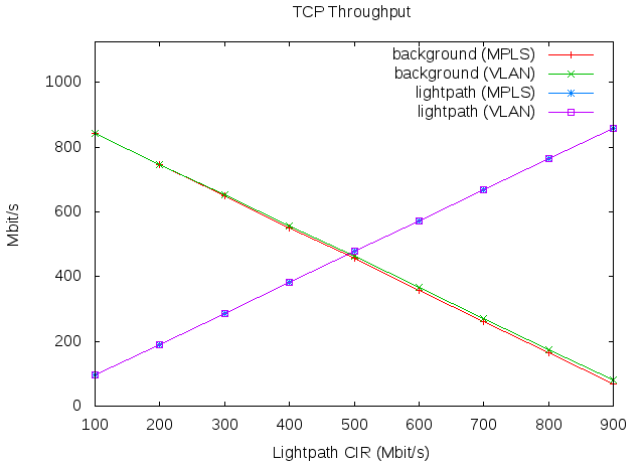


Figure 4.13. *Scenario 3, test 4–12.* TCP throughput – comparing background and lightpath traffic based on a VLAN and MPLS configuration, showing negligible difference between a VLAN or MPLS configuration

High Priority Lightpath – with Congestion

Figure 4.14 and figure 4.15 show the RTT and jitter performance of the MPLS and the VLAN configuration, when both are transmitting UDP packets at 1 000 Mbits/s; which is twice the amount of the available resources. Figure 4.14 shows how the RTT of the background traffic increases when the configured CIR value is higher. For all configured CIR values, the background traffic is offering more traffic than the network is able to serve. Consequently, the buffers will fill up completely, regardless of the configured CIR value. However, the number of packets in the buffer does not determine the RTT value on their own. When more and more resources are assigned to the lightpath traffic (by increasing the CIR value), less resources are available for the background traffic. While the arrival of background traffic stays high — still resulting in full buffers — the service time available for background traffic decreases, which results into longer queueing time. Hence, the RTT values for the background traffic increase.

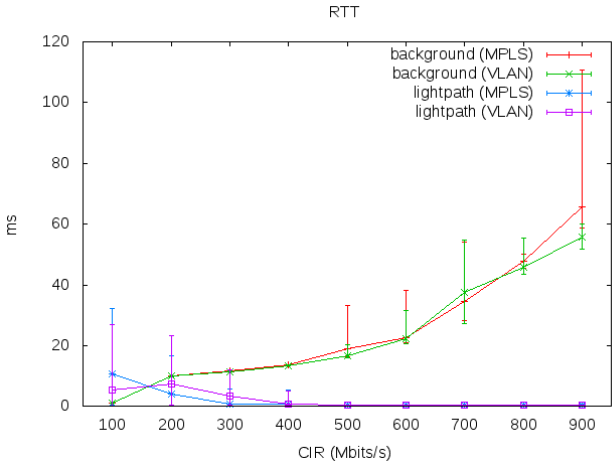


Figure 4.14. *Scenario 3, test 13–21 and Scenario 4, test 10–18.* RTT values – comparing background and lightpath traffic based on a VLAN and MPLS configuration. Background RTT is slowly increasing with a higher CIR value for the lightpath traffic. For both lightpaths, the RTT shows very low values.

Regardless of the configured CIR value, the lightpath traffic is also transmitting excessive amounts of traffic. All lightpath packets not within the configured CIR value are dropped due to traffic policing. The remaining packets (within CIR configuration) are queued for service, right after the current job in service according to a nonpreemptive priority scheduling strategy. This should result in steady and low RTT values, regardless of the configured CIR value. However, the lightpath traffic does experience elevated RTT values at the lower CIR configurations. Unfortunately, detailed information from the network device could not be retrieved, which made it impossible to examine this behavior extensively. For example, it could be useful to investigate the CPU load when high number of packet drops occur. Overall, the VLAN and MPLS configuration perform alike, and the difference between them is negligible.

Figure 4.15 shows the jitter results of the aforementioned experiments. As mentioned already above, excessive traffic is dropped by means of traffic policing and the remaining packets (within CIR configuration) are queued for service, right after the current job in service according to a nonpreemptive priority scheduling strategy. However, the lightpath traffic does experience elevated jitter values at the lower CIR

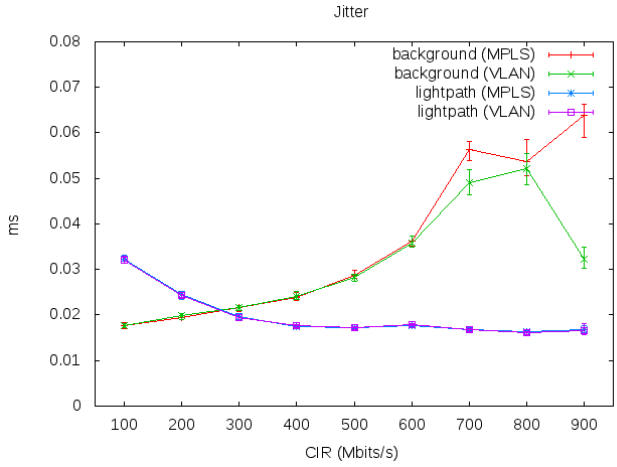


Figure 4.15. *Scenario 3, test 13–21 and Scenario 4, test 10–18.* Jitter values show increasing jitter values for the background traffic, while lightpath traffic decreases and stabilizes just below 0.02 *ms*.

configurations. When CIR values increase, jitter decreases for the lightpath traffic, and stabilizes just below 0.02 *ms*. A direct cause for this observation could not be indicated, although at roughly the same CIR configurations, the RTT shows a similar trend which could indicate a possible relation.

The background traffic on its turn is able to gain all the remaining resources. At lower CIR configurations the background traffic is experiencing less jitter than the lightpath traffic. However, the trend of the background traffic is inverted compared to the lightpath traffic; the higher the CIR, the higher the jitter becomes. At higher CIR configurations, the lightpath is gaining more resources while being served with SP scheduling. This causes more response time variation for background traffic upon arrival. This trend holds for the background traffic up to 800 Mbits/s. Higher transmission speeds show a slightly improving VLAN background jitter. The MPLS jitter resumes its previous trend.

Overall, the MPLS configuration is showing equal results compared to VLAN, especially for the lightpath traffic. The MPLS and VLAN background traffic show similar results, but at higher transmission speeds they start to diverge a little. In general, jitter values are low for both VLAN and MPLS transport.

High Priority Lightpath – without Congestion

In a real-world scenario, lightpath traffic is only initiated or permitted when the network is able to assign enough resources to the lightpath connection without disrupting background traffic. To improve resource availability, a buffer is used in this scenario. The lightpath traffic is transmitting UDP packets 50 Mbits/s below the configured CIR value, and the background traffic (also UDP) with 950 Mbits/s minus the configured CIR value. This results in two times a buffer of 50 Mbits/s. Figure 4.16 and figure 4.17 are considering RTT and jitter under these less stressed scenarios.

Figure 4.16 shows slowly increased RTT values with higher CIR values for the lightpath traffic (both MPLS and VLAN configuration). With increased CIR values, the average time that lightpath traffic needs to wait for a packet being served also increases. The RTT values of the background traffic decreases and stabilizes until a CIR value of 800 Mbits/s (also for both, MPLS and VLAN configuration). At a CIR value of 900 Mbits/s the RTT of the background traffic is significantly increasing.

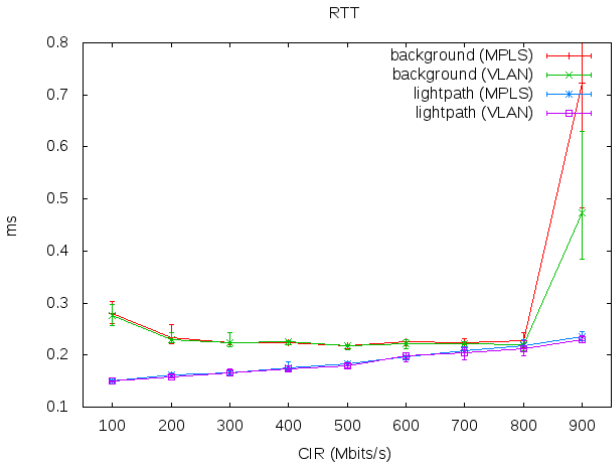


Figure 4.16. *Scenario 3, test 22–30 and Scenario 4, test 19–27.* RTT values show low values for background and lightpath traffic when transmissions do not exceed available resources. Only near to maximum transmissions show increased RTT values for the background traffic.

Jitter results are shown in figure 4.17. The jitter values for the lightpath traffic slowly increases until a CIR value of 500 Mbits/s. After a small improvement it starts to increase again at 800 Mbits/s. More unexpected is the jitter of the background traffic. When the lightpath is configured using a VLAN configuration, the jitter increases in value until the CIR is configured at 700 Mbits/s, after which it improves down to a value lower than the lightpath traffic. When a MPLS configuration is used, the same jitter values for the background traffic are observed, except for a CIR value of 900 Mbits/s, where jitter varies a lot, and is significantly worse. Overall, jitter values are very good and both configurations perform alike.

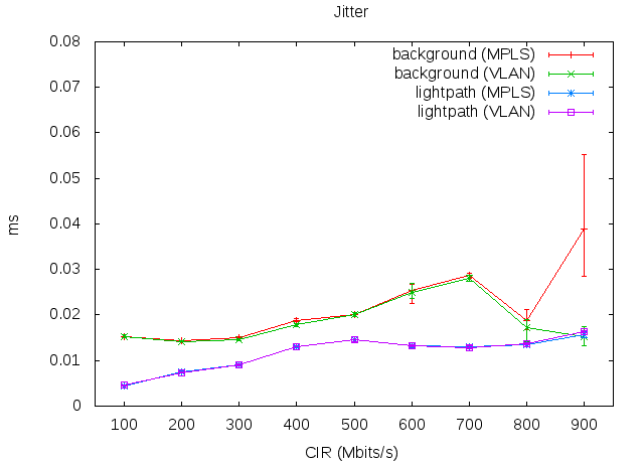


Figure 4.17. *Scenario 3, test 22–30 and Scenario 4, test 19–27.* Jitter values show slowly increasing jitter values for both lightpath types. Unexpected jitter behavior is observed for background traffic.

Chapter 5

Conclusion

This thesis reports an empirical study on the extension of lightpath services on last-mile packet-switched networks, such as a campus network infrastructure, in order to gain insight on how lightpath connectivity can be provided. This chapter starts with answering the research questions, after this, results are discussed and suggestions for future work are given.

The first research question addressed the effects on the transmission characteristics of lightpath transmissions on last-mile infrastructures technologies. Results revealed that last-mile infrastructure technology is able to provide the same transmission characteristics as a physical dedicated lightpath. However, the intermediate network devices of the last-mile lightpath take account for some additional delay. But, for the end-user's experience this added delay is negligible.

When a last-mile infrastructure is used, a small dissimilarity was observed for the maximum throughput. This is caused by different overhead of the chosen transport technology (i.e., datalink layer and possibly additional tunneling technique). This may have practical implications for applications in demand of high throughput, such as radio astronomy. These applications should take into account if the chosen transport technology is able to serve the needed bandwidth. If not, using lightpath transmission over last-mile infrastructure may not be sufficient enough. In these cases, either a different transport technology, or a physical dedicated lightpath should be considered.

The second research question considered a shared infrastructure (i.e., routed traffic and dynamic lightpath using the same hardware), examining the consequences for the lightpath and the existing background traffic. Results show that when lightpath con-

nectivity is provided over a last-mile best-effort infrastructure, resources are shared among other traffic. Hence, a lightpath connection is not isolated from background traffic, resulting in interference between lightpath and background traffic. This indicates that using a shared infrastructure may lead to nullifying the property advantages of a lightpath connection. It was also observed that background traffic may suffer from high speed lightpath transmission. In both cases, this occurred especially when a non-congestion controlled protocol is used in combination with a congestion controlled protocol (e.g., UDP and TCP respectively). TCP reacts on the network condition and holds back on transmission in an attempt to mitigate packet-loss. UDP does not react on the network conditions. Therefore, when high rate UDP traffic is transmitted, the TCP congestion control mechanism will reduce throughput significant and large impact will occur.

The third research question examined if QoS is required to provide or improve lightpath connectivity (i.e., performance guarantees of a lightpath) in the last-mile network. When a best-effort infrastructure is used, results show that resource sharing is not controlled. Based on these findings it can be argued that network administrators are in need to have more control on network traffic which justify the usage for QoS techniques. QoS allow network administrators to determine the level of interference between lightpath and background traffic, while guaranteeing minimum amount of services. If and how much interference is allowed between lightpath and background traffic is up to the network administrator. A trade-off must be made between the guaranteed properties of a lightpath and the user-experience of the best-effort background traffic.

The characteristics of a end-to-end connection can be graded depending on the application used. Real-time applications are more demanding compared to 'normal' data transmission, but the minimal requirements can still vary significant. Haptic devices demand delays of $<50\ ms$, jitter of $<2\ ms$, and packet loss of $<10\%$. Voice can handle more jitter and delay, but require packet loss of $<1\%$ [49]. Based on the minimal requirements of these real-time applications, the results of this study show very good results; considerably lower compared to the above mentioned requirements.

Overall, using QoS techniques to provide high priority packet-switched lightpath with resource allocation reveals promising results for lightpath connectivity on last-mile networks. Additional, MPLS tunneling technique is able to provide a good solution when tunneling is required.

5.1 Discussion and Future work

In this report, the deployment of lightpaths in the last-mile network infrastructure is considered. In particular, the extension of a lightpath offered by the NREN at the demarcation point. The performed experiments show that a last-mile infrastructure is sufficient to realize a lightpath connection up to the end-user. However, results show that on a best-effort network, background and lightpath traffic can interfere severely with each other which nullify the guaranteed properties of a lightpath. This also holds vice versa; lightpath traffic can have high impact on background traffic.

To gain more control on the interference between background and lightpath traffic, QoS techniques can be used. This allows the lightpath traffic to preserve its properties to the detriment of the background traffic.

How much the background traffic may suffer from lightpath connectivity was not part of the research goal in this thesis. Currently, this is not automated yet, and therefore needs to be determined by the network administrator. A trade-off must be made between best-effort user experience and the guaranteed properties of lightpath connectivity. In this thesis, a strict priority scheduling assuring the lightpath properties in combination with resource limiting (traffic policing) is investigated. The results revealed good control for this combination on the amount of interference between traffic. Usage of a Network Resource Manager (NRM) to management and orchestrate lightpath connectivity is not addressed in this thesis, but is expected to be useful to assist the network administrator by automating this configuration process and improve network utilization.

Last-mile networks rarely consist of solely layer2 networks, but usually comprise of a layer3 IP-switched, or a combination of layer2 and layer3 networks. Therefore, in many cases a tunneling technique is required to realize a layer2 lightpath from the demarcation point up to the end-user. MPLS is a technology which has been largely positioned for use in core networks, the question therefore arises if MPLS would provide a good performing tunneling solution for last-mile infrastructures. The results from this thesis show that MPLS is a good performing technique, thus able to provide a good tunneling solution for lightpath connectivity.

The experiments conducted in this work are performed using iperf. Iperf is a traffic generation and measurement tool. Using iperf for this purpose provides good insight in the end-to-end performances. However, not only the network, but also the end-stations' hard- and software is included in the iperf measurements, resulting in a coarse granularity measuring approach. Result showed that the end-node's performance may

have an increasingly important role, when the achievable limits are explored.

During the experiments, high speed UDP transmissions show unexpected low throughput measurements. Tests performed afterwards indicate a performance issues at the operating system, more investigation is needed to determine the exact cause. Future experiments should take this issue into account. This could be realized by excluding high transmission flows. If this is undesirable, a hardware traffic generator is recommended.

Only Constant Bit Rate (CBR) traffic is considered during the experiments. Using more realistic transmission patterns is expected to result in to more realistic results. However, from the analysis of the obtained results it is also expected that using more realistic data would not change the outcome of this research. Investigating behavior under more realistic packet length and inter-arrival times to confirm this hypothesis is subjected to future work.

This study provided valuable information as a first step into the extension of lightpath connectivity. The next step for lightpath connectivity in the last-mile infrastructure will be dynamic lightpaths. Overall, this study shows that the extension of lightpath connectivity into the last-mile is feasible as an alternative for dedicated physical lightpaths. Practically, QoS must be provided to assure lightpath properties and to control background and lightpath interference.

Bibliography

[1] AutoBAHN. http://www.glif.is/meetings/2012/tech/slides/20121012-BoD-Lessons.pdf.

[2] Automated GOLE Pilot project. http://wiki.glif.is/index.php/Main_Page.

[3] Geant testbeds. http://www.geant.net/Innovation/Testbeds/Pages/Home.aspx.

[4] Geni. http://www.geni.net/.

[5] Global Lambda Integrated Facility. http://www.glif.is.

[6] Iperf. http://iperf.sourceforge.net/.

[7] openDRAC. https://www.opendrac.org/.

[8] Science dmz network architecture. http://en.wikipedia.org/wiki/Science_DMZ_Network_Architecture.

[9] tcpreplay. http://tcpreplay.synfin.net/wiki/tcpreplay.

[10] Virtual Circuits (OSCARS). http://www.glif.is/meetings/2012/tech/slides/20121012-oscars.pdf.

[11] Role of Open Exchanges in the evolution of global research and education networking "Open Network for Open Science". http://www.glif.is/publications/papers/20110519BStA_Open_Exchanges.pdf, 2011.

[12] Science dmz. http://fasterdata.es.net/science-dmz/, 2013.

[13] I. F. Akyildiz, T. Anjali, L. Chen, J. C. De Oliveira, C. Scoglio, A. Sciuto, J. A. Smith, and G. Uhl. Invited a new traffic engineering manager for diffserv/mpls networks: Design and implementation on an ip qos testbed. *Comput. Commun.*, 26(4):388–403, Mar. 2003.

[14] B. Arnaud, E. Bos, and I. Monga. GLIF Architecture Task Force - DRAFT GREEN PAPER. http://www.glif.is/publications/papers/GLIF-Architecture-Green-Paper-01-2013.pdf, 2013.

[15] R. Biesbroek. Literature study on dynamic lightpaths - the current state of art. 2013.

[16] A. Bill St. Open science, science as a service and open lightpath exchanges. http://billstarnaud.blogspot.nl/2011/05/open-science-science-as-service-and.html, 2011.

[17] S. Blake, D. Black, M. Carlson, and et al. RFC 2475: An Architecture for Differenctiated Services, 1998.

[18] S. Boele, P. de Boer, I. Idziejczak, B. Kreukniet, R. van der Pol, and F. Dijkstra. Virtual Routing and Forwarding for Ligthpaths - Implementations at SARA. https://noc.sara.nl/nrg/publications/VRF_Implementations_at_SARA.pdf, May 2011.

[19] Z. Bojovic, E. Secerov, and V. Delic. Qos testing in a live private ip mpls network with cos implemented. *Comput. Sci. Inf. Syst.*, 7(3):529–549, 2010.

[20] R. Braden, D. Clark, and S. Shenker. RFC 1633 : Integrated Services in the Internet Architecture: an Overview, 1994.

[21] R. Braden, L. Zhang, S. Berson, and S. Herzog. RFC 2205: Resource ReSerVation Protocol (RSVP), 1997.

[22] M. Campanella, A. Sevasti, R. Krzywania, K. Stamos, V. Reijs, D. Wilson, and C. Tziouvaras. Bandwidth on demand services for european research and education networks. In *Bandwidth on Demand, 2006 1st IEEE International Workshop on*, pages 65–72, 2006.

[23] B. Constantine, G. Forget, R. Geib, and R. Schrage. Framework for TCP throughput testing. RFC 6349, RFC Editor, Fremont, CA, USA, Aug. 2011.

[24] E. Dart and J. Metzger. The science dmz. http://www.es.net/assets/Uploads/20110201-dart-science-dmz.pdf, 2011.

[25] P. Dekker and R. Spoor. The missing link between nren and iaas. https://tnc2012.terena.org/getfile/986, 2012.

[26] DICE Control Plane Working Group. Inter-Domain Controller (IDC): Interoperable Control Planes for Dynamic Circuit Networks. http://www.controlplane.net.

[27] A. K. Erlang. The Theory of Probabilities and Telephone Conversations. *Nyt Tidsskrift for Matematik*, 20(B):33–39, 1909.

[28] GEANT. GN3-JRA2T2_LastMileSolutions_v3.2.doc. http://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-JRA2T2_LastMileSolutions_v3.2.doc.

[29] J.-P. Georges, T. Divoux, and E. Rondeau. Strict priority versus weighted fair queueing in switched ethernet networks for time critical applications. In *Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International*, pages 141–141, 2005.

[30] Global Lambda Integrated Facility. Connecting research worldwide with lightpaths GLIF Automated GOLE Pilot Project. http://www.glif.is/meetings/2011/winter/poster/AutoGOLE-handout-20110217-v5.pdf, 2011.

[31] X. Huang, Y. Lin, W. Wang, and S. Cheng. Qosjava: An end-to-end qos solution. In *Proceedings of the 8th International Conference on Management of Multimedia Networks and Services*, MMNS'05, pages 302–313, Berlin, Heidelberg, 2005. Springer-Verlag.

[32] W. Huisman. When simplicity becomes complex - on the road to a scalable and dynamic surfnet7 network. http://surf-academy.nl/media/SURFnet%207%20In%20Depth/2013_06_SN7%20in%20depth_Wouter%20Huisman.pdf.

[33] Internet2. The network development and deployment initiative: Expanding the breadth and reach of internet2 network service through the development of the open science scholarship, and service exchange. http://www.internet2.edu/network/ose/docs/Open%20Science%20Exchange%20Whitepaper.pdf, 2011.

[34] F. Le Faucheur, B. Davie, S. Davari, and et al. RFC 3270: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, 2002.

[35] L. Momtahan and A. Simpson. Switched lightpaths for e-health applications: a feasibility study. In *Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on*, pages 469–472, 2006.

[36] I. Monga. Ecsel leverages openflow to demonstrate new network directions. http://esnetupdates.wordpress.com/2011/11/04/ecsel-leverages-openflow-to-demonstrate-new-network-directions/, November 2011.

[37] K. Nichols, S. Blake, F. Baker, and D. Black. RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 1998.

[38] V. Olifer. Different Flavours of VPN Technology and Applications. https://www.ja.net/sites/default/files/Different%20Flavours%20of%20VPN%20Technology%20and%20Applications.pdf.

[39] Open Grid Forum. Overview - NSI WG - Open Grid Forum. http://redmine.ogf.org/projects/nsi-wg.

[40] G. Z. Papadopoulos. Experimental assessment of traffic generators. http://georgiospapadopoulos.com/MScThesis.pdf, July 2012.

[41] J. Phuritatkul, K. Nguyen, M. Koibuchi, Y. Ji, K. Fukuda, S. Abe, J. Matsukata, S. Urushidani, and S. Yamada. Investigating qos performance on a testbed network. In *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 1267–1272, 2007.

[42] F. Pujol. Mobile traffic forecasts 20102020 & offloading solutions. http://www.ict-befemto.eu/fileadmin/documents/publications/workshop_2011/F._PUJOL_IDATE_15_05_2011.pdf.

[43] N. Rouhana and E. Horlait. Differentiated services and integrated services use of mpls. In *Computers and Communications, 2000. Proceedings. ISCC 2000. Fifth IEEE Symposium on*, pages 194–199, 2000.

[44] SKA Organisation. The square kilometer array. http://www.skatelescope.org/.

[45] SURFnet. Nieuwe dienst gekoppeld aan surfconext: Greenqloud. http://www.surfnet.nl/nl/nieuws/Pages/NieuwedienstgekoppeldaanSURFconextGreenQloud.aspx, November 2012.

[46] Universiteit Twente. Detailed Proposal Universiteit Twente. http://www.utwente.nl/sb/uim/infrastructuur/UT_Campus_Challenge.pdf, 2013.

[47] V. C. Valgenti. *Dynamic content generation for the evaluation of network applications*. PhD thesis, Pullman, WA, USA, 2012. AAI3517443.

[48] J. Wang and Y. Levy. Managing performance using weighted round-robin. In *Computers and Communications, 2000. Proceedings. ISCC 2000. Fifth IEEE Symposium on*, pages 785–792, 2000.

[49] K. M. Yap, A. Marshall, and W. Yu. Providing qos for distributed haptic virtual environments in ip networks. In *Proceedings of the First International Conference on Immersive Telecommunications*, ImmersCom '07, pages 13:1–13:6, ICST, Brussels, Belgium, Belgium, 2007. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[50] Y. Zhang, P. Chowdhury, M. Tornatore, and B. Mukherjee. Energy efficiency in telecom optical networks. *Communications Surveys Tutorials, IEEE*, 12(4):441–458, 2010.

List of Figures

List of Tables