Dynamic Topology Adaptation enabled by Network Virtualization: A Use-Case for the Future Internet

Thomas Zinner*, Dominik Klein*, Sebastian Meier‡, David Wagner‡,
Marco Hoffmann†, Wolfgang Kiess§, Vlad Singorzan¶, Matthias Schmid¶
* University of Würzburg, Chair for Communication Networks, Würzburg,Germany
† Nokia Siemens Networks Management International GmbH, Munich, Germany
‡ Institute of Communication Networks and Computer Engineering (IKR), Universität Stuttgart, Stuttgart, Germany
§ DOCOMO Communications Laboratories Europe GmbH, Munich, Germany
¶ Infosim GmbH & Co. KG, Würzburg, Germany

I. Introduction

The current Internet has evolved during the last decade to a global provider of various new services like social networks, cloud applications, or web and email. However, the underlying structure of the Internet has not evolved in the same pace and is somewhat inflexible. In particular, it is hard to introduce new network services with certain quality of service (QoS) requirements. In addition, the future Internet will also face challenges like a rising number of mobile users connected via wireless links or real-time services with high bandwidth demands. However, the Internet architecture is still bound to its best effort basis and not able to satisfy these demands.

Network Virtualization (NV) reduces time and overhead of resource adaptation and allows to consolidate networks on a functional level and differentiate them on a service level. In such a future Internet, a multitude of virtual networks (VNs) will coexist and complement each other. These coexisting networks allow specialization but require isolation of functionalities to provide dependable and predictable networks.

The objective of the Control and Management of Coexisting Networks (COMCON) project is to design novel control and management mechanisms that support the coexistence of VNets in a future networking scenario and to illustrate their economic advantages. To that end, COMCON addresses a couple of challenges that have not been sufficiently considered by existing approaches. This includes network operation issues, the support of arbitrary network technologies, technology migration and reuse considerations, and traffic management with respect to the perceived service quality. More information on the reference architecture as well as on the interaction between the Application Service Provider (ASP), the Virtual Network Operator (VNO), the Virtual Network Provider (VNP) and the Physical Infrastructure Provider (PIP) can be found in [1], [2].

The reminder of this abstract is structured as follows. In Section II, we give details about the monitoring and operation, Section III describes the set up of our demonstration.

II. Operation and Monitoring

During the operation phase of a VN, it needs to be monitored, controlled, and adapted to changing requirements, e.g. an increasing customer base of a running application. Each functional role (PIP, VNP, VNO, ASP) comprises measurement agents within its components. These measurement agents gather information about the component state and accumulate this knowledge into a monitoring database. A decision component (DC) examines that information and decides on further actions like ordering additional resources, changing or optimizing the network operation or claiming SLA violations.

In previous work [2], [3], we discussed three different control and monitoring patterns that can be hierarchically combined:

- Horizontal Control Loops
- Vertical Control Loops triggered by upper layers
- Vertical Control Loops triggered by lower layers

In the following, we first explain the horizontal control loop in general and then, how it is utilized in our demonstration.

A. Horizontal Control Loops

In the operation phase, each functional role (PIP, VNP, VNO, ASP) has a control component, a DC, and a monitoring component. With these three components the role is able to manage its resources and fulfill the agreed SLAs. Based on obtained monitoring data, the DC can instruct the control component to trigger certain actions. The result of the actions is perceived by the monitoring component. As an example in our demonstration, the horizontal control loop of the VNO is utilized to maintain the user-perceived quality of a customer of a video streaming service. The necessary building blocks in that case are a QoE monitoring component and the control and decision components.

B. QoE Monitoring Component

For the optimization of VNs with respect to the user-perceived quality, it is important to provide means for measuring and monitoring this quality. The monitoring in the network needs to be aware of the application for which the VN should be optimized. In our scenario, we use video streaming via the scalable video codec (SVC) as application running in the VN. In principle, a middlebox could use deep packet inspection to discover the necessary information from the SVC header. However, this information is not sufficient to calculate the user-perceived quality with a certain accuracy. Hence, we

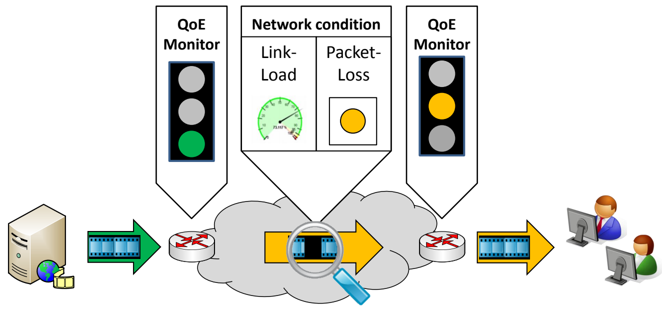

Fig. 1. QoE Monitoring Agent System

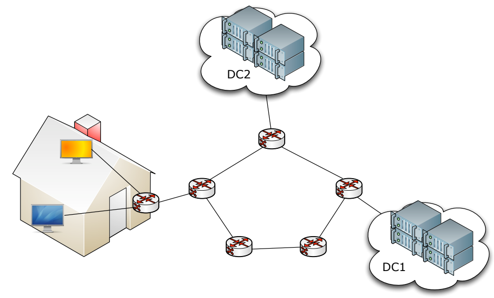

Fig. 2. Considered Demo Scenario

introduce a new shim header between the UDP header and the application data. In this header, we include the necessary information like the frame number, the number of packets for this frame, and the type of the frame. In addition to this information provided in the shim header, the middlebox also has detailed knowledge about the video, in particular its inter-frame dependencies. This information is important as a received frame may depend on other frames and can only be decoded if all required frames have been received correctly. If at least one required frame is missing, it can not be decoded and the perceived quality of experience at the end user is negatively influenced and needs to be adapted accordingly. Eventually, the calculated QoE measurements are collected by the agent system of StableNet [4] and visualized, e.g. with a traffic light signal. StableNet is a service assurance platform which provides fault and performance management in enterprise or telco environments. A sketch of the QoE monitoring can be seen in Figure 1.

C. Control and Decision Component

Based on the collected QoE measurement data of the agent system of StableNet, the decision component of the VNO can instruct the control component to trigger certain actions. These actions may range from increasing the bandwidth on a possible bottleneck link to adapting the VN topology. The first option is only possible if the VNO has free resources available at the bottleneck link. Otherwise, this would require an interaction with its VNP via a vertical control loop. The second option, adapting the VN topology, is mainly possible in two ways. The first way would be to select another source for the video streaming service and hence avoid the bottleneck link. The other way would be to use multiple paths between the source and the destination. In our SVC scenario, this could be achieved by sending the different layers over different paths. The decision which action should be executed is done by the decision component which is in our case the business unit of the VNO.

III. Demonstration Scenario

In the demonstration, we focus on a small network scenario with several edge and intermediate virtualized network nodes, cf. Figure 2. We consider a video-on-demand ASP delivering its content to the end customers from a data center providing cloud platform-as-a-service infrastructure. The ASP contracts a data delivery service with a VNO, which therefore reserves virtual network links between the data center and the customers. Due to an increase in the customer base, the virtual networks extends its resources on the same links and later on also acquires virtual resources on other links to meet the demand of the service. When the customer base keeps increasing and eventually exceeds a certain threshold, it becomes necessary to integrate an additional data center to guarantee the quality of the service.

The demonstration also covers the negotiation phase between the functional roles based on a standardized network description in an extended Shared Information/Data (SID) model from the TM Forum [5]. We also extend the scenario by including virtual machines, which are directly attached to MPLS tunnels. This demonstrates the feasibility of seamless integration of virtual hosts with virtualized links providing guaranteed QoS. It also allows the virtual topology to differ significantly from the physical one while guaranteeing negotiated properties of virtual links. The extended demonstration deployment now also includes a GMPLS-capable of-the-shelf router showing the advantage of using standardized and well-established technologies for virtualization.

IV. Acknowledgments

This work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 01BK0917, Förderkennzeichen 01BK0918, G-Lab). The authors alone are responsible for the content of the paper.

References

[1] M. Duelli, S. Meier, D. Wagner, T. Zinner, M. Schmid, M. Hoffmann, and W. Kiess, “Experimental Demonstration of Network Virtualization and Resource Flexibility in the COMCON Project,” in *8th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, Thessaloniki, Jun. 2012.
[2] D. Schlosser, M. Duelli, T. Zinner, S. Meier, D. Wagner, M. Barisch, M. Hoffmann, W. Kellerer, and M. Schmid, “Service Component Mobility Enabled by Network Virtualization,” in *Euroview 2011*, Aug. 2011.
[3] S. Meier, M. Barisch, A. Kirstädter, D. Schlosser, M. Duelli, M. Jarschel, T. Hoßfeld, K. Hoffmann, M. Hoffmann, W. Kellerer, A. Khan, D. Jurca, and K. Kozu, “Provisioning and Operation of Virtual Networks,” *Electronic Communications of the EASST, Kommunikation in Verteilten Systemen 2011*, vol. 37, Mar. 2011.
[4] Infosim GmbH & Co. KG, “Stablenet,” http://www.infosim.net, 2012.
[5] TMForum, http://www.tmforum.org, 2012.