Network Planning, Control and Management Perspectives on Dynamic Networking

Thomas Michaelis[(1)], Michael Duelli[(2)], Mohit Chamania[(3)], Bernhard Lichtinger[(4)], Franz Rambach[(1)], Stefan Türk[(5)]

[(1)] Nokia Siemens Networks GmbH & Co. KG, Munich, Germany - Research Technology & Platforms, thomas.michaelis@nsn.com

[(2)] Julius-Maximilian University of Wuerzburg, Germany - Institute of Computer Science, Chair of Distributed Systems

[(3)] Technical University Carolo-Wilhelmina of Braunschweig, Germany - Institute of Computer and Network Engineering

[(4)] Leibnitz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities, Garching, Germany

[(5)] Dresden University of Technology, Dresden, Germany - Chair for Telecommunications

Abstract *We motivate that network planning, service provisioning and restoration, as well as service management need to be investigated and aligned at large in order to realize dynamic networking.*

Introduction

The continuous bandwidth cost decline witnessed in the past decades, most notably fuelled by technological progress and market competition, provides an economic context which drives the creation of novel services and the growth of traffic. Network operators have to cope with this circumstance against the backdrop of decreasing revenues per bit/s, especially in times of a global economic downturn.

Dynamic networking is one viable approach to keep traffic cost in balance with revenues: It implies a certain level of automation which can substantially reduce cost for recurring operational transactions (OPEX), and it can also improve revenue collection by re-using infrastructure for more users and by providing services on demand as a differentiating feature.

The remainder of this paper highlights three key aspects of dynamic networking which need to be addressed in order to facilitate dynamic networking paradigms, namely network planning, service provisioning/restoration, and service management.

Network Planning

The task of network planning is to provide control and management mechanisms with a sufficient amount of networking resources. Therefore, hardware configurations are computed based on current as well as forecasted traffic and failure scenarios to design the network.

a. Network Design & Survivability

The calculation of these hardware configurations implies different perspectives. For customers, network design has to ensure the requirements stipulated with network providers in *service level agreements* (SLA), like *quality of service* (QoS) guarantees, and mainly affects the data plane. For network providers, network design also has to respect additional traffic caused by network failures, management, and control mechanisms. In case of multi-layer networks, multiple technologies, their services, and corresponding control mechanisms have to be evaluated which makes cost efficiency regarding *total cost of ownership* (TCO) more complex [1].

While control and management traffic does not contribute significantly to the total traffic demand, backup paths can easily increase the required capacity by more than a factor of two over the original capacity requirements [2]. Since most technologies in a multi-layer network can react in case of failures, control mechanisms have to determine which layer starts the recovery for a specific failure. This choice concerns recovery time as well as the number of affected data flows. Assuming non-cooperating control mechanisms, failures affecting a certain layer cannot be detected on lower layers in a multi-layer network which are not affected. Hence, protection on multiple layers is required which implies the coordination of different resilience mechanisms, so called *escalation strategies* via additional control mechanisms.

For *dynamic* network provisioning, the success of network design not only requires reliable traffic forecasts and failure probabilities but also has to allocate additional spare capacity at the right spots to cope with unforeseen traffic loads which is in a direct trade-off to low TCO. So network design provides the basis for control and management mechanisms which have to utilize the given and unchangeable resources at their best. Also, efficient network migrations strategies must be available to change network configurations when upgrading active networks to ensure minimal active service interruptions.

b. Network Migration

To ensure that an existing network configuration is able to carry future traffic loads, suitable migration strategies are required. The goal of these strategies is

978-3-8007-3173-2 © VDE VERLAG GMBH

to find cost optimal solutions detailing the insertion time and the hardware upgrade or replacement mechanism in a currently operational network.
During network migration, budget restrictions as well as time-dependent factors like hardware prices, energy cost, and reselling of existing equipment have to be respected. Additionally, SLA penalty payments have a significant impact on the migration order [3].
A common migration approach is the installation of new devices in parallel to existing structures [4]. This yields a kind of overlay topology into which new demands can be integrated one by another without interruption of existing services.
In *dynamic* network provisioning, migration strategies have to adapt to constantly changing network situations. Therefore, the integration of new hardware in an existing management plane is more suitable. The network management system then has to aggregate running as well as new services. Such transitions require suitable control and management mechanims to prevent SLA penalties and guarantee cost optimal solutions.

Service Provisioning & Restoration

In general, there are two options for establishing services and reacting to failures: Manual service provisioning via the management plane or automated service provisioning via the control plane. On the one hand it should always be possible to configure, control and manage the network and provisioned services via the *management plane* (MP). On the other hand these tasks can also be realized on an automated control plane, which shows its strengths especially in multi-layer and multi-domain scenarios.

a. Automatic Provisioning & Restoration

Automatic (or on demand) provisioning enables client network elements to trigger a call setup, based on standardized *user-network interfaces* (UNIs). The call is subsequently realized by one or more connections in the provider network.
Today, distributed intelligence based on *Generalized Multi-Protocol Label Switching* (GMPLS) is the de-facto set of standards for dynamic provisioning and restoration on the basis of a distributed control plane.
Dynamic provisioning and restoration could also be realized on the management plane, but management systems tend to be single vendor and proprietary. In contrast, multi-vendor compatibility on the control plane even extends automatic provisioning and restoration to multi-vendor and multi-provider contexts. As a prerequisite, standardized *network-network interfaces* (NNIs) are needed.
Automatic restoration provides a high level of survivability in connection with automatic protection mechanisms on the same layer and, if appropriately coordinated, with survivability mechanisms on other layers. The latter implies a coordinated planning of the layers, which is often termed *multi-layer optimization* (MLO).
Actually, key drivers for first GMPLS deployments in core transport networks were the provided second line of defense against multiple failures and less resource consumption for survivability purposes. Nowadays, control plane scalability in the IP/MPLS layer of large multi-layer networks is another important driver. A GMPLS deployment in core/transit nodes enables interworking with IP/MPLS edge nodes and thus avoids a logical full mesh network on the IP/MPLS layer.
In transparent optical networks, restoration mechanisms may today require a couple of minutes to provide a backup connection for technological reasons (settlement of control loops along the selected backup route in response to power increase). Thus in absence of all-optical counter-measures on the system level, subsecond response times can only be achieved in higher - electrical packet or circuit switching - layers. The advent of 40G and 100G transmission systems based on coherent reception and extensive receiver-side *digital signal processing* (DSP) will likely impose additional constraints on restoration mechanisms: first, the response time will probably be extended by the DSP synchronization delay, and second, the DSP's dispersion compensation capability - which is related to implementation complexity and cost - will limit the length of the backup route.
Networks based on meshed topologies typically seen in metro core and core networks can have multiple paths between two endpoints, and thus would benefit significantly from automatic provisioning and restoration mechanisms. In virtual star topologies where only two alternative paths between two endpoints are available, this is not the case. Thus metro access and metro aggregation areas are less qualified for control plane deployment.

b. Path Computation

Fast and efficient multi-layer and multi-domain path computation is an integral building block for operating and controlling dynamic networks and efficiently establishing services. This operation is currently done either via the management plane, i.e. centrally inside of *network management systems* (NMS), or via the control plane inside each *network element* (NE) using e.g. OSPF or CSPF. The usage of the *Path Computation Element* (PCE) concept, which can belong to the MP and/or to the CP, is another option which is emerging as the de-facto solution for multi-domain and multi-layer dynamic path computation. In the following section, we focus on this solution.
A PCE “is an entity that is capable of computing a network path or route based on a network graph” [5]. The PCE can compute optimal constrained multi-layer and multi-domain paths and as the PCE interface

has been standardized, the PCE is inter-vendor, multi-domain and multi-layer capable. Since only the interface is standardized, the internal routing algorithm executed by the PCE is not restricted by any constraints, i.e. any propriety or standardized algorithms can be deployed inside a PCE.
For multi-layer path computation many different PCE architectures exist, e.g. one central entity which has knowledge about all the layers or multiple PCEs with or without inter-PCE communication. More details about the categorization and the advantages/disadvantages of the different approaches can be found in [6]. By using the PCE concept advanced and time consuming MLO algorithm, which uses the network resources efficiently, can be executed.
Along a pre-specified domain chain, where the domain chain can be pre-configured or obtained via routing protocols, the PCE architecture can compute optimal constrained paths. The lack of transit *traffic engineering* (TE) information available in existing protocols such as BGP makes them unsuitable for supporting multi-domain QoS routing, and different proposals have extended existing topology aggregation mechanisms as well as BGP to introduce TE parameters for QoS routing. Other approaches such as time/threshold triggered inter-domain routing advertisements are also commonly used which trade-off accuracy of routing information for frequency of inter-domain signaling, which governs the scalability of inter-domain routing systems. In recent works [7,8], we have explored the possibility of increasing the scalability and stability of inter-domain topologies by reducing the frequency of inter-domain advertisements while advertising accurate information by reserving additional resources in the data plane exclusively for inter-domain transit traffic, and adaptively controlling the reserved capacity for inter-domain traffic to improve link utilization over traditional data plane partitioning schemes. The capacity is reserved in the form of pre-reserved LSPs between border nodes in an Ethernet domain and effectively forms a stable virtual mesh-based overlay topology used exclusively for transit traffic.

Service Management

Management plane functions can be subdivided into service management, network management and element management, respectively, which work in a hierarchical configuration. Thus a *service management system* (SMS) with an interface for customer self-services is provided in every provider network, acting on top of the NMS.

a. SMS-NMS Interworking

On receiving a request for a new service, the SMS determines the network resources required to provision the service request and requests them from the NMS. So the SMS essentially maps services and network resources.
Therefore the SMS and the NMS need a common information model for network resources and services and how they can be mapped together.
After the setup of a new service the SMS has to monitor the performance of the service and to react proactively, if the service level specifications of the SLA may be violated. For the end-to-end monitoring of service *operations, administration and maintenance* (OAM) functions are defined. These comprise of functions for fault detection and location, performance monitoring and end-to-end testing. Such functions are standardized for many technologies, like SDH, OTN, Ethernet, MPLS-TP.

b. Multi-Domain Service and Performance Management

An organizational model defining the interactions between different domains is needed to provision a service spanning multiple domains. Such a model defines the structure of management processes for *failure, configuration, accounting, performance and security* (FCAPS) management between the participating domains.
The organizational model also influences the composition of SLAs for inter-domain services, which depend on the mutual SLAs defined by different neighboring domain pairs.
The OAM functions can also be used for end-to-end monitoring of inter-domain services as they are realized as in-band functions. The OAM standards define hierarchical levels of OAM management domains to separate the OAM packets from operator, provider and customer. With such OAM mechanisms the operator is not required to disclose the internal network topology, because the OAM packets of higher management domains pass the lower domains transparently.

Conclusions

In this paper, we highlight network planning, service provisioning/restoration, and service management as prerequisites for dynamic networking:

First, network planning and the migration to the resulting network setup provide the degrees of freedom for agile network operation.

Second, service provisioning and restoration are the functions required to bring services into being, and to keep them alive upon failures. In the past, the former functionality was solely realized on the management plane. An implementation on an additional control plane is desirable for automatic topology discovery and multi-layer and multi-domain path computation, while the PCE framework enables the straightforward and interoperable extension of path computation to multi-provider scenarios.

978-3-8007-3173-2 © VDE VERLAG GMBH

Finally, service management is responsible for appropriate support of the end-to-end service level by the involved providers.

Our conclusion is that all of these aspects need to be investigated and aligned at large (see Fig. 1) in order to make dynamic networking a reality. We are currently targeting these three aspects in a joint European CELTIC project in which researchers from networking and signal processing are collaboratively working on dynamic network provisioning in survivable multi-layer networks with high data rates up to 100 Gbit/s.

Acknowledgement

This work has been performed in the framework of the CELTIC subproject 100GET-E3 (Project ID CP4-001), and it is partly funded by the BMBF (Project IDs 01BP0740, 01BP0771, and 01BP0775). The authors would like to acknowledge the contributions of their colleagues from Nokia Siemens Networks, Julius-Maximilian University of Wuerzburg, Technical University Carolo-Wilhelmina of Braunschweig, Dresden University of Technology, and Leibnitz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities.

References

1 M. Duelli, E. Weber, M. Menth, "A Generic Algorithm for CAPEX-Aware Multi-Layer Network Design," 10. ITG-Fachtagung Photonische Netze, Leipzig, Germany, 2009.

2 C. Pluntke, M. Menth, M. Duelli, "CAPEX-Aware Design of Survivable DWDM Mesh Networks," IEEE ICC, Dresden, Germany, 2009.

3 Verbrugge, S.: "Strategic Planning of Optical Telecommunication Networks in a Dynamic and Uncertain Environment," University of Ghent, 2007

4 Kiy, N.: "Carrier-Ethernet: Transportnetz für Next Generation Networks", VDE ntz 3-4, 2009

5 A. Farrel, J.-P. Vasseur, J. Ash, “A Path Computation Element (PCE)-Based Architecture,” IETF RFC 4655

6 E. Oki, Tomonori Takeda, J-L Le Rou, A. Farrel, “Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering,” IETF Draft, work in progress, draft-ietf-pce-inter-layer-frwk-10.txt

7 M. Chamania, X. Chen, A. Jukan, F. Rambach, C. Gruber, M. Hoffmann, "Adaptive Advance Reservation Based Inter-Domain Framework," IEEE ANTS 2008, Bombay, India, Dec 2008.

8 M. Chamania, X. Chen, A. Jukan, F. Rambach, C. Gruber, M. Hoffmann, "Embedding Optical Ethernet Services within the Path Computation Element Framework: The 100GET Approach," Technical Digest of Optical Fiber Communication Conference 2009 (OSA/OFC 2009), San Diego, CA, March 2009.

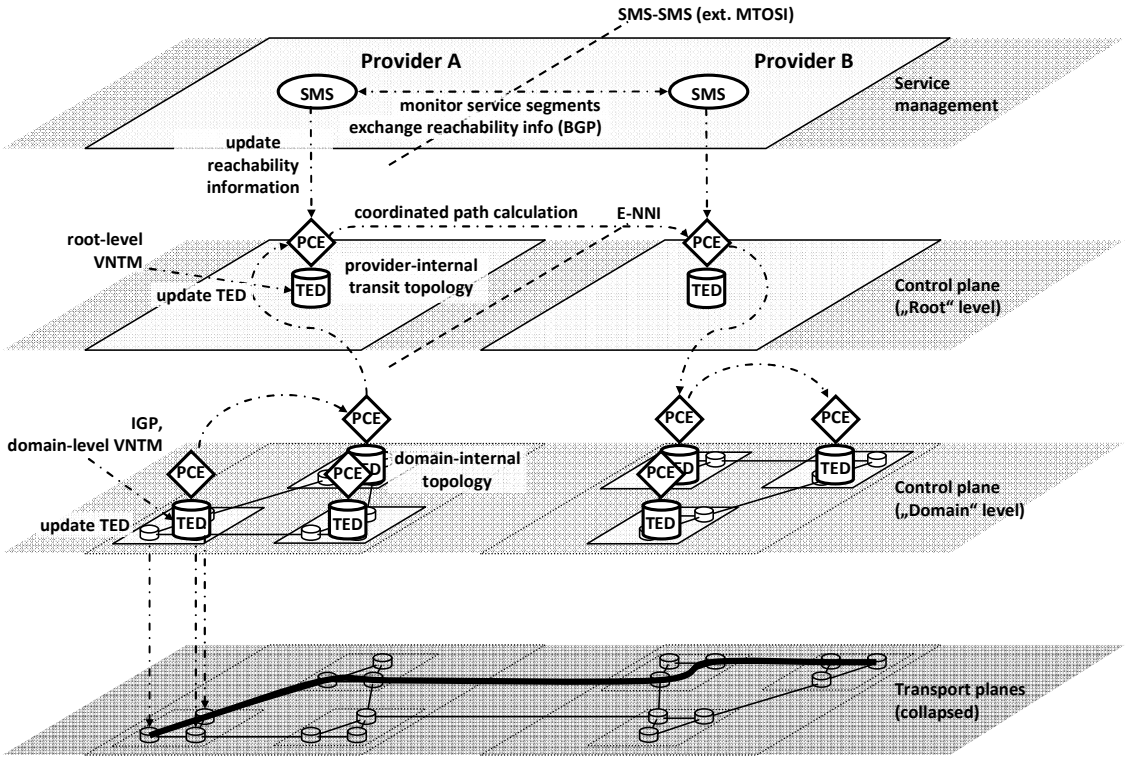

Fig. 1 - An example architecture based on control plane and PCE functionality. Network planning forms the transport planes (bottom), service provisioning and restoration across layers, domains and providers is in the responsibility of a hybrid PCE approach (middle), and service management ensures adequate QoS end to end (top).