

Towards Dynamic Virtual Private Service Networks: Design and Self-Management

Zakaria Benahmed Daho and Noemie Simoni
Computer Science and Networks Department
GET/ENST/ LTCI-UMR 5141 CNRS
Paris, 46 rue Barrault
75634 Paris Cedex 13, France

Abstract—The aim of this paper is to propose a solution for service virtualization and structure within what we call the Next Generation Service (NGS) context. For this purpose, we first propose to distinguish services from networks by separating the network level and the service level. Afterwards, we propose to generalize and apply networking concepts within the service level. This leads us to introduce the necessary elements to support service virtualization, i.e. Virtual Private Service Networks (VPSNs) and Virtual Service Networks (VSNs). The VPSN is the private network that translates the logic of the service required by the user and proactively maintains the end-to-end QoS to meet the Service Level Agreement. The VSNs provide means to support the VPSNs using self-management capabilities to anticipate the local QoS degradation and take the necessary preventive actions.

Keywords—*Next Generation Service, Service Virtualization, Virtual Private Service Network, Virtual Service Network*

I. INTRODUCTION

In today's dynamic information society, emerging technologies continue their rapid progression, making possible new and improved applications and services. The evolution of these services and applications is progressing in parallel with that of telecom networks. While telecom networks are moving towards the Next Generation Networks (NGNs), services and applications also have to evolve towards what we can call the Next Generation Services (NGSs). Dynamic contexts and new services offered by peer-to-peer, virtual topologies and ambient networks will be supported by the NGSs.

In this context, managing and maintaining services and applications according to the required Quality of Service (QoS) pose new challenges. Current management solutions depend mainly on the underlying network management capabilities to maintain and manage services and applications. They do not provide all the required service solutions and some service problems (service capacity, processing delay, etc.) can not be dealt with by the network. Moreover, reacting on time to these problems and customers' needs is a key requirement to ensure service continuity, QoS maintenance and thus customers' satisfaction within our context.

Towards this end, we have to separate services from networks and to introduce self-management capabilities within the service level. Important work is being done in this field. Intelligent network [1], TINA [2], web services [3] and recently the service overlay networks [4] distinguish service and network

levels. This separation is confirmed also in management standards as in the TeleManagement Forum where the eTOM [5], which distinguishes service management from network management, it proposed. However, this is not sufficient to share services, to fulfill dynamic service (re)deployment and to be more efficient to maintain service QoS within dynamic context. This is why we aim to create two autonomous synergic layers (service and network layers) where there are sharable and self-managed “networked elements” that fulfill autonomously their specific tasks. The self-management is QoS-driven and the whole collaborates to maintain proactively the end-to-end QoS of the requested service in a transparent manner regarding the user that is, the virtualization of services.

To achieve this and thus to meet the needed proactivity and service architecture flexibility, we propose to apply networking concepts within the service level (§II). A first result concerning this application consists of creating the Virtual Private Service Network (VPSN), the architecture of the new application within the NGS context (§III). To maintain the QoS of the VPSN, we propose the Virtual Service Network (VSN) concept (§IV), another important result of applying networking concepts within the service level. The VSN is the self-management support of the VPSN QoS. The fulfillment of the VPSN dynamicity will be discussed in section §V. Conclusion and perspectives are given in the last section.

II. APPLYING NETWORKING CONCEPTS WITHIN THE SERVICE LEVEL

By applying networking concepts in the service level, we mean to have an analogy between well-known and proven networking concepts (QoS, flows, routing) and those of the service level that we aim to propose in this paper. This leads to achieving the needed synergy between the service and the network [6] as well as flow traceability. As a first result of this application, we have to consider two sub levels within the service level as shown in figure 1.

While the upper sub-level (of the service level) represents the service requested by the user that is the whole application (end-to-end provided service), the lower sub-level represents the elements that support the application that is, the whole sharable applicative resources provided to support the user applications. This separation distinguishes the user's point of view of the service from that of the provider's. The whole contributes to service virtualization.

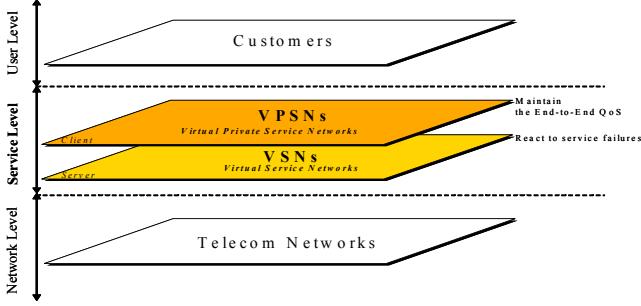


Figure 1. Our proposed 3-leveled Architecture: User, Service, Network

Our new vision of the user applications consist in considering networked service components instead of having monolithic service architectures [7]. As within the network level we find networked entities that constitute telecom networks, we propose within the service level that networked service components constitute Virtual Private Service Networks (VPSNs). This network is virtual because of the nature of the applicative resources and service components that are sharable as well as the provided abstraction feature. This network is private because it is the response to the service request of a particular customer having specific QoS needs. The aim of the VPSN is to satisfy the end-to-end contracted QoS. Details about the VPSN are presented in section §III.

To support the VPSN, we introduce a new concept that translates the provider's view of the service level. This sub-level provides the necessary service components to the VPSN to perform the required tasks. These components correspond to the sharable applicative resources that are obtained thanks to applying networking technology within the service level, which allow the design of Virtual Service Networks (VSNs) formed by functionally equivalent service components. The VSNs are the self-organizing networks that aim to dynamically provide an alternative service component to replace the failed component within the VPSN. Thanks to the VSNs, the VPSN dynamicity is fulfilled. Details about the VSN are presented in section §IV.

III. THE END-TO-END SERVICE: THE VPSN

The VPSN is constituted by two main architectural elements: the VPSN nodes (service components) (§III.1) and the VPSN links (§III.2) that connect the VPSN nodes. The VPSN (§III.3) translates the logic of the requested service and must provide the right end-to-end QoS and proactively maintain this QoS to meet the customer's SLA. The role of the QoS model for proactivity and self-management is discussed in section (§III.4).

III.1. The VPSN Nodes

The VPSN node is the architectural element that is responsible for fulfilling a specific processing function. This processing constitutes part of the end-to-end processing that the VPSN will provide. Each VPSN node provides its functionalities through well defined interfaces: server interfaces and client interfaces. With the server interfaces, the node will be able to answer the requests. With the client interfaces, the node will be able to send requests and notifications.

III.2. The VPSN Links

The VPSN links are virtual architectural elements that are responsible for transmitting and supporting the VPSN node interactions and service-level messages. These interactions are fulfilled within a service session between the VPSN nodes. The VPSN links thus define temporary relationships among the VPSN nodes. The lifetime of these links depends on the VPSN lifetime and on its use. The fulfillment of the VPSN link transmission functionality depends on the effective localization of the nodes to be connected. This fulfillment can thus be done directly among the interacting nodes or by using the connectivity capabilities of the underlying level (the network level).

III.3. The VPSN

To build the VPSN that will meet the customer request, we must identify and then select the right VPSN nodes, regarding their processing functionality and QoS, and establish the right VPSN links, regarding their communication capabilities and QoS, that connect the selected nodes. Identifying the required VPSN nodes means finding which nodes are necessary to carry out the VPSN processing and thus the customer requested service functionalities. This is done thanks to service profiles that are created for each offered service by the service supplier. Among the identified nodes, we have to choose which one can carry out the requested behavior. This service node selection must be carried out in parallel with the link establishment to connect the selected nodes. We will see in section §IV the role played by the VSNs for service node selection. The VPSN uses the logic that specifies how the selected nodes must be connected according to the semantic of the requested service. The link establishment is thus carried out according to the VPSN logic. We call "semantic routing" the process of linking the VPSN nodes according to a precise logic.

III.4. The Role of QoS for Self-Management

To allow the proactive control of the end-to-end VPSN QoS, we propose to integrate behavior (QoS) information within each VPSN element. That means that, the VPSN nodes as well as the VPSN links must be aware of the QoS that they have to provide (local contracts) and the QoS that is currently being provided (current behavior). To maintain proactively the current QoS conforming to the local contracts, we propose to provide the VPSN elements with QoS threshold values. These threshold values translate the limit of the normal processing (or communication) behavior of the nodes (or of the links) under normal conditions. As soon as the current QoS exceeds the threshold values, this indicates an impending QoS processing or communication problem and a fast reaction is required. The QoS is evaluated thanks to four generic criteria: Delay, Availability, Reliability and Capacity. Each criterion is evaluated thanks to measurable parameters. Therefore, the end-to-end VPSN QoS depends on the QoS of its nodes as well as on the QoS of the network that support the VPSN links. The end-to-end VPSN QoS is obtained by active measurement. These measurements are scalable because they are performed by the probes in precise points where the VPSN nodes are deployed. This allows the VPSN to get the information about the behavior of the networks that support the VPSN links. To

avoid system oscillations and to converge to the SLA, the behavior of each element must be in conformity with engineering rules that are determined by the service provider. These rules translate for example the adequate parameter setting of the QoS thresholds values, the measurement frequency, the neighborhood, etc.

We have thus used the same QoS model (four criteria with current, contracted and threshold parameters for each criterion) for the VPSN as well as for its elements from their design phase.

IV. A SUPPORT SERVICE: THE VSN

As mentioned in section §II, we want the VPSN to share the applicative resources (service components), i.e. applicative resources are made available for use by the VPSNs. The resource sharing is between service components with the same functional features, i.e. they are functionally equivalent. The functionally equivalent service components constitute VSNs where each VSN is responsible for providing service components to replace a failed one within the VPSN.

As we need equality between the service components to satisfy resource sharing and to provide a dynamic reaction to services failures, we propose to adopt peer-to-peer as a means to provide these features. Thus peer-to-peer relationships evolve within each VSN. In this case, the VSN service nodes are peer entities and constitute peer communities (VSN can be seen as a peer community). Each community is responsible for offering a specific type of service node (Figure 2).

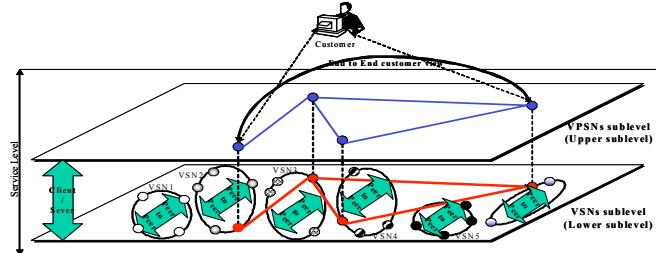


Figure 2. A detailed view of the service level structure

Taking into count the QoS within the VSNs is important because the VPSN has to choose a service node with the right behavior to constitute the whole user application. The community QoS aspect must thus be taken into account. To that end, we propose to characterize each community by a contract so that each node that belongs to a VSN adheres to the community contract. The latter describes the common functional characteristics to ensure the functional equivalence of the VSN nodes as well as the common quality characteristics to ensure that the service nodes fulfill their related functions with a minimum guaranteed quality. The VSN quality characteristic is expressed according to our QoS model. Each community contract acts as an identifier for each VSN, since it specifies the functional characteristics of the provided nodes within the community as well as the QoS characteristics that the entire service nodes must respect.

The adopted VSN structure offers two main advantages. The first advantage concerns the maintenance of the VPSN. As each node is a member of a precise VSN, replacing a “faulty” service

node and finding an equivalent one is done rapidly, the VSN is identified and the requested node is rapidly found thanks to the adopted peer-to-peer VSN structure. The second advantage concerns the creation of the VPSN and more precisely the service node selection. In fact, to search for a service node with a desired QoS and functionality, we have first to identify its related VSNs. Once a corresponding VSN is found, a search within this VSN is performed. Thanks to the VSN structure, this search will be fulfilled rapidly.

Like the VPSNs, the VSNs are structured into nodes and links. Since the VSN nodes are peer entities, the VSN links support peer-to-peer exchanges between these nodes. Unlike the VPSN links, the VSN links do not depend on the existence or not of VPSNs. The relationship between VSNs and VPSNs can be expressed as following. While the VSN maintains its community as well as supporting the VPSN by providing the required service nodes, the VPSN traces a path (semantic routing) by selecting the provided service nodes to meet the customer request. VSNs and VPSNs thus fulfill autonomous processing.

To each VSN, we associate a table (VSN table) to store the necessary information about the organization of the community as well as about its members (ID, QoS, status, etc.). The VSN tables must be updated dynamically to cope with the dynamic changes within the communities. Associated with the VSN tables, a peer-to-peer protocol will be necessary for service node search and community maintenance. While within the VPSN the semantic routing depends on the requested service, the VSN peer-to-peer protocol depends only on its community. As the service node deployment is independent from network routing, the network can find another path to support the applicative exchanges after the VSN has replaced the faulty VPSN node. Therefore, the VSN can offer more possibilities and abilities to the VPSN to resolve service-level problems than a solution that remains on the network-level routing capabilities. In fact, the VSN will allow the rerouting of the VPSN node exchanges and interactions towards other nodes for example that are able to respect their QoS contract. It will thus play a capital role to resolve VPSN node failures.

V. FULFILLING THE VPSN DYNAMICITY

The VPSN have to satisfy the end-to-end QoS to meet the customer’s SLA and to satisfy its requirements. To that end, we propose to control the conformity of the QoS at each VPSN processing step. As soon as the evaluated QoS goes beyond its threshold values, the VPSN will take preventive actions necessary to maintain its end-to-end QoS.

For the QoS self-management, the VPSN checks continuously its current QoS values compared to its QoS thresholds values. The VPSN current QoS values are obtained by measuring current performance of the actually used nodes and links (i.e. the current workflow). If before the end of the VPSN processing, the VPSN current QoS goes beyond the threshold values, it means that the local adaptations carried out by the actually used nodes and links did not succeed. In this situation, the VPSN has to deal with the remaining nodes and links that did not yet started their processing to avoid end-to-end QoS degradation.

To do so, the VPSN has to renegotiate the contract for the unused nodes and links (i.e. finding other nodes and links with other contracts). The idea behind this proposal has been applied within the telecom network [8]. In fact, if a path does not give satisfaction to guarantee the network QoS, its contract is renegotiated. This leads to a redirection of the flows to enable them to guarantee the QoS. This technique inspired us to propose the VPSN end-to-end dynamicity where the change of network path corresponds to the change of the VPSN nodes and links. The VPSN nodes are changed thanks to the VSNs. Changing the VPSN links means negotiating a new communication contract with the underlying telecom network.

Having to deal with the VPSN nodes and links implies combining the service level processing capabilities (for the nodes) as well as the network level communication capabilities (for supporting the links). This means that the two levels have to collaborate to satisfy the VPSN needs of processing and communication with a given QoS. If the network can not provide the communication support with the right QoS, the VPSN seeks other nodes to compensate the lost QoS of the link. The final aim is to satisfy the requested QoS by using either service level capabilities or network level capabilities or both. This collaboration can be carried out only if we have the same concepts (QoS, model, etc.) on the network level as well as on the service level ensuring the flow traceability between these two levels. This service/network synergy is missing within the existing solutions mainly because they are either in overlay, or depend on the network. In our proposal, we are neither completely dependent nor independent of the network, but rather integrated and complementary to carry out the necessary collaborations. The QoS and its model are the synergy drivers.

The dynamic behaviors of the VPSN must be carried out rapidly during its usage. Therefore, we must reduce the elapsed times between the proactive detection and the VPSN reaction. To that end, it is necessary to automate and to perform both the service management and control functionalities during the VPSN usage. This means that we must guarantee the synergy and the collaboration of the service control, the service management and the service usage plane.

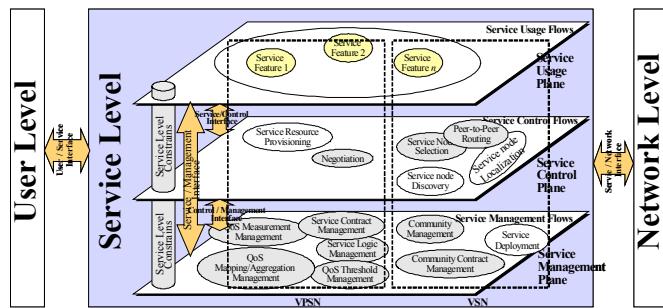


Figure 3. The organization of VPSN and VSN functionalities within the service level

This synergy is materialized by taking into account both management and control functionalities within all the proposed elements of the service level: VPSNs, VSNs, service nodes and links within the NGS context. This means that each Service Level Element (SLE) must encompass, in addition to its core functions, its management as well as its control functionalities.

This leads us to propose the structure model of these SLEs where the management and control are both taken into account. It is for this reason that each SLE can be seen as an autonomous and self-managed element within the NGS context. Figure 4 shows our proposed model to structure the SLEs.

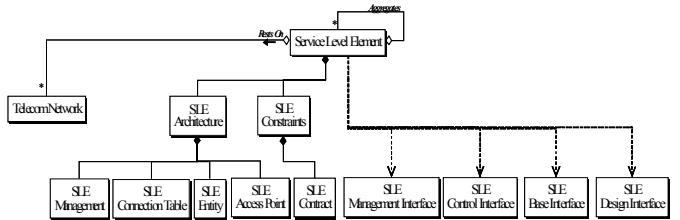


Figure 4. The Service Level Element Model within the NGS context

This proposed model shows that each SLE has four interfaces: management, control, base and design interfaces. Each SLE has its own contract. The architecture of the SLE is described thanks to four classes: management, entity (Core functions), connection table and service access point.

VI. CONCLUSION AND FUTURE WORK

Within the NGS context, each service (or application) will adopt a network structure (VPSN) with the autonomy and proactive reaction capabilities and self-maintenance of its QoS. The advantages of our proposal can be summarized as follows: (i) the dynamic networked view of the service level is obtained thanks to the VPSN and the VSN structures. (ii) The QoS is natively supported within the SLEs. The same QoS model is adopted whatever the SLE. (iii) The SLEs maintain proactively their QoS while current solutions act and take corrective actions only after detecting the problem. (iv) The service/network synergy is guaranteed. The whole contributes to service virtualization.

This proposed structure creates a new field of investigations, a new context, which we named NGS for which efficient and generic protocols need to be found as well as informational models to continue working on self-management. Our future work is articulated around these last points on both a theoretical and a practical (experimentations) level.

REFERENCES

- [1] B.Martini, F.Baroncelli, P.Castoldi, "A novel service oriented framework for automatically switched transport Network", IEEE/IFIP IM 2005.
- [2] <http://www.tinac.com/specifications/specifications.htm>
- [3] Sahai A. et al. "Automated SLA monitoring for web services", IEEE DSOM, October 2002.
- [4] Z.Li, P.Mohapatra, "QRON: QoS-Aware Routing in Overlay Networks", IEEE JSAC, 2004.
- [5] GB921, "enhanced Telecom Operation Map", TMF Document, April 2005
- [6] R.Keralapura, N.Taft, G.Iannaccone, C-N.Chuah, "Can ISPs and Overlay Networks form a Synergistic Co-existence?", IEEE/IFIP DSOM, 2004.
- [7] L.Erlkh, "Leveraging Legacy System Dollars for E-Business", IEEE IT Pro, 2000
- [8] F.Bennani, N.Simoni, "Dynamic management for end to end IP QoS : from best-effort to personalized services", Terena Networking Conference, 2000.