Network Sharing in the Next Mobile Network: TCO Reduction, Management Flexibility, and Operational Independence

Ashiq Khan, Wolfgang Kellerer, Kazuyuki Kozu, and Masami Yabusaki, DOCOMO Communications Laboratories Europe GmbH

ABSTRACT

Mobile network operators, with decreasing revenue but high network performance requirements, are standing at a crossroads. Investing in 3GPP defined highly functional mobile networks and the consequent maintenance to sustain the market-driven network service quality standard results in high total cost of ownership unseen in fixed operators. Revenue reduction will make it significantly difficult to fund such TCO in the future. In this light, sharing networks is a viable solution to reduce network expenditure, as can also be seen from present trends. However, current networking sharing solutions, although reducing TCO, come with limitations in network management flexibility, and standalone decision making in network expansion and service introduction. Virtualization-based isolation techniques have the potential of enabling network sharing along with management flexibility and independence among the sharing entities. However, virtualization brings added complexity to the overall network management structure. In this article, we propose a next mobile network architecture, where the physical network infrastructure is shared by multiple entities, but the management and control of the physical infrastructure, virtual network creation and maintenance, and the usage of the virtual networks are decoupled from each other to reduce management complexity in each segment. In addition, we address the technical as well as business perspectives of the proposed architecture, discuss open issues, and provide research directions to realize such a flexible value-added commercial network for the future.

INTRODUCTION

One of the most apparent challenges for future mobile networks will be the handling of the predicted increase in mobile traffic volume [1]. Figure 1 presents the dramatic increase in global mobile traffic over the next five years, especially in the domain of video and web traffic. To make this traffic increase a reality, and to harvest the underlying business opportunity, this traffic growth has to be mastered without increasing network costs in terms of both capital expenditure (CAPEX) and operational expenditure (OPEX). Current mobile network operators fully own and exploit their network infrastructure. Full ownership allows for the freedom and flexibility of control and management of the network. However, huge human and financial efforts are invested in order to correctly plan and deploy the network equipment, configure and maintain it, and finally operate it in order to provide the required network services to the end customers. With the deployment of different access and core technologies (e.g., Universal Mobile Telecommunications System [UMTS], Long Term Evolution/Evolved Packet Core [LTE/EPC]) [2], which require changes in the access and/or core network, the cost pressure on the mobile operators greatly increases, in terms of both CAPEX and OPEX. At the same time, ever increasing client demands in terms of network resources and heterogeneity of deployed services, each with its special requirements, add to the strain of a network operator. While these demands have been addressed so far by network overprovisioning, the diminishing return on investment (ROI) and the inherent inefficient use of resources of such solutions increase the operator's financial burden.

As a natural consequence, a new viable business model emerges in which two or more mobile operators share a common network infrastructure. This reduces deployment and operation costs, and decreases the time to market [3]. Market surveys suggest that different types of network sharing solutions are currently deployed by over 65 percent of European mobile operators. These solutions bring cost savings of up to 40 percent in terms of CAPEX, and up to 15

0163-6804/11/$25.00 © 2011 IEEE

percent in terms of OPEX over a five-year period [4]. Similar surveys predict that network sharing solutions will be preferred by 60 percent of mobile operators worldwide when it comes to deploying LTE in the coming five years.

While network sharing solutions are already available, as either standardization efforts or concrete vendor products [5], they do not fully address the requirements of future mobile operators. Such requirements include extending the scope of sharing, increasing the isolation/separation in both the data and control planes among operators, along with the privacy and security of their operations, and increasing the flexibility and dynamicity in accommodating different service-oriented operators with special requirements (e.g., in-network processing).

The purpose of this article is to introduce a new network architecture for flexible and dynamic network sharing among multiple network operators. Our architecture model is based on a connected, end-to-end physical infrastructure that can be fully shared with the help of network virtualization technologies. The isolation properties of the virtualization technology help us expand the scope of network sharing (Fig. 2), increase the operators savings in terms of total cost of ownership (TCO), and address the requirements of future sharing solutions. It ensures the flexibility and freedom of network operation, which conventional sharing schemes fail to provide.

The contributions of this article are fourfold:

- We present a survey on existing network sharing solutions. We classify these solutions, and analyze the advantages and challenges facing mobile operators deploying them,
- We extend the scope of the network sharing paradigm by presenting a set of advanced requirements on the fourth generation (4G) and beyond next mobile network (NMN) [6]. These requirements are based on mobile traffic and service trends, and on emerging mobile technologies.
- We propose an NMN architecture that fulfills the identified requirements with a view on network sharing by means of virtualization, and discuss potential technologies for implementing it.
- Finally, we discuss the open issues related to our proposal, identifying ongoing and future areas of research.

Current Network Sharing Solutions

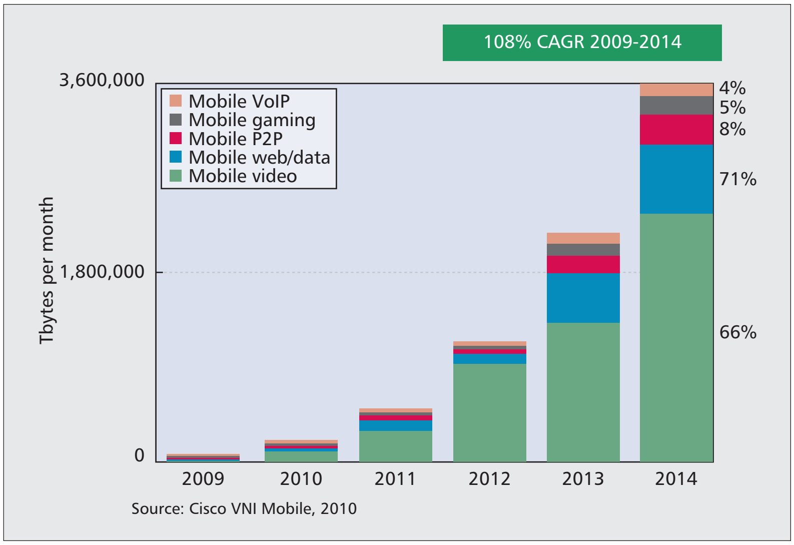
Network sharing reduces deployment and operation costs, and decreases the time the operators need to bring new technologies to customers [3]. Network sharing can be viewed from two perspectives: geographical and technical [5].

Geographical Classification

From the geographical point of view, network sharing can take various aspects depending on the business model intended and the already independently covered areas by the involved mobile operators.

The dimensions of network sharing can be characterized as:

Standalone: Two or more network operators own and control their respective physical network infrastructure. No network sharing or interaction between operators exists (outside roaming agreements).



Source: Cisco VNI Mobile, 2010

Figure 1. *Cisco global mobile traffic predictions 2009–2014, and application traffic split.*

Full split: Each operator covers a specific non-overlapping geographical region, and each operator extends its own area of operation by using the other operator's network. This scenario is interesting for operators of similar strengths who want to enter roaming agreements to extend their network coverage.

Unilateral shared region: One mobile operator has full control over the network infrastructure in one region, and a new greenfield operator enters the market by utilizing this existing infrastructure. This model lowers the barrier for new business entrants, and allows existing operators to better capitalize on their installed resources. This is the present mobile virtual network operator (MVNO) model.

Common shared region: two operators of similar size want to have a presence in the same region, but they still decide to share the infrastructure. This scenario is mostly attractive in rural areas where the estimated revenues are lower, so operators need to carefully plan their investment.

Full sharing: Two or more mobile operators decide to fully share their network, either access, core, or both, in order to render the operations and management of the network more efficient.

Technological Classification

From the technological point of view, network sharing solutions today mostly concentrate on the access network, which is the most costly part of a mobile operator's network. The range of solutions encompasses:

Passive radio access network (RAN) sharing: This implies the collocation and sharing of sites for antenna towers. Two or more mobile operators decide to install their own antennas/base stations at the same sites and share the costs for site construction and renting. Possibly the tower site operations and construction can be outsourced to third party companies.

Sharing solutions might need the involvement of a trusted third party, which installs and operates the shared infrastructure, and acts as a broker among the sharing operators. Such a solution comes at the cost of losing some of the operational control of the network operators, and re-organization of the involved departments.

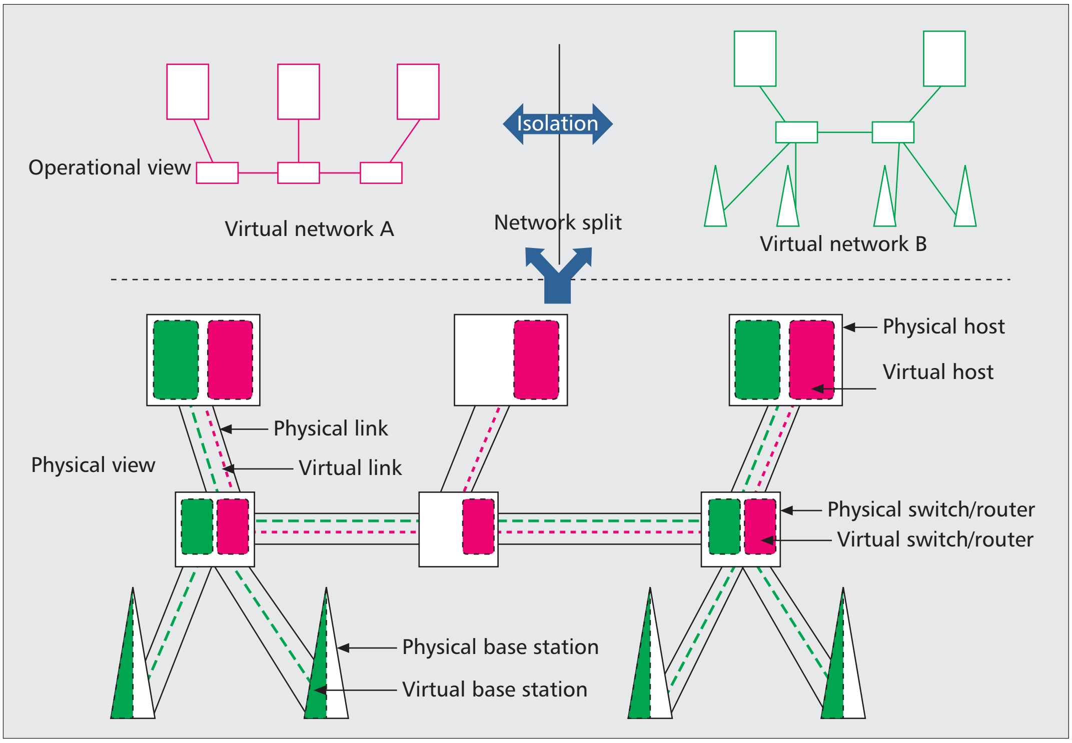


Figure 2. *Network splitting and mutual isolation by virtualization.*

Active RAN sharing: This implies two or more mobile operators sharing the same antennas/base stations. The operators can pool together their spectrum resources and operate them in parallel according to predetermined resource allocation agreements. The Third Generation Partnership Project (3GPP) standardizes the necessary procedures for such operations in [2] as the RAN is the primary focus of 3GPP. The other parts of the network can be shared by present transport technologies (e.g., IP forwarding).

Roaming based sharing: When one network operator relies on another operator's coverage on a permanent basis. The two operators can decide to either share only the access network, pool spectrum resources or not, or extend the sharing to some parts of the core network. A detailed list of network sharing solutions, together with their characteristics, can be found in Table 1.

Advantages and Challenges

Table 2 summarizes the main advantages and challenges of current network sharing solutions. The main advantages, as discussed before, concentrate around the reduction of CAPEX/OPEX for the mobile operators (infrastructure cost, deployment cost, operations cost, maintenance and energy costs). Operators can improve their cost efficiency and better utilize the available network resources. Furthermore, sharing solutions can lead to improved perceived network and services quality by extending an operator's coverage or increasing its capacity. They can also allow operators to focus on their core competencies and business focus, by outsourcing infrastructure relevant operations. All these advantages can help an operator to better position its business in the overall competitive environment.

On the other hand, deploying network sharing solutions can be challenging for the involved mobile operators. Besides the explicit implementation of the desired technical solution with the attendant cost, operators must also take into account regulatory issues, which might differ from country to country. At the same time, the operation model must be updated, and some of its aspects need synchronization with the sharing partners. This involves an extra degree of risk, and might need adjustment in the operator's business strategy, both short and long term. Finally, sharing solutions might need the involvement of a trusted third party, which installs and operates the shared infrastructure, and acts as a broker among the sharing operators. Such a solution comes inherently at the cost of losing some of the operational control of the network operators, and re-organization of the involved departments.

The Next Mobile Network Evolution and Promising Technologies

The mobile cellular network is a fast moving network compared to the Internet. NTT DOCOMO, INC. introduced 3G in Japan in 2001 with a downlink bit rate of 384 kb/s. It has introduced LTE/EPC in 2010 with a downlink bit rate of 300 Mb/s. This represents an increase in bit rate of almost 750 times in 9 years. As the projected target of NMN deployment is 2020, we anticipate that 5 Gb/s and above will easily be available in the RAN (Fig. 3). The architecture of NMN is primarily based on the requirements derived from such high bit rates in the RAN part. Below, we briefly describe the most impor-

Sharing solution	Type of sharing	Details	Features
Site sharing	Passive	Operators collocate their own equipment	Very simple; does not require operational coordination; support equipment may or may not be shared
Tower sharing	Passive	Operators share the same mast, or rooftop	Operators have own antennas, huge CAPEX reduction, environment benefits
Spectrum sharing	Active	Parts of spectrum is leased by one operator to another	Improve spectrum efficiency, fights spectrum scarcity
Antenna sharing	Active	Antenna and all related connections are shared	Passive site elements are shared too
Base station sharing	Active	Operators maintain control over logical Node Bs	Can operate on different frequencies, fully independent
RAN sharing	Active	RAN resources are combined: antennas, cables, BS and transmission equipment	Separate logical networks and spectrum
RNC sharing	Active	RNC physical resources are shared	Operators maintain logical control over the RNC
MSC and router sharing	Active	MSCs and SGSNs are shared	Regulatory and technical hurdles, becomes attractive with IMS
Backhaul sharing	Active	Transport is shared, e.g., fiber	Regulatory issues, good for rural areas
Roaming	Active	Operator networks located in separate geographical regions	Pool geographical regions to expand user coverage
MVNOs	Active	Virtual operators lease the infrastructure from another operator	Based on wholesale agreements

Table 1. *Present network sharing solutions: details and features.*

tant planes of NMN: the advanced mobile access (AMA), optical mobile network (OMN), and service delivery network (SDN), along with the promising future component technologies.

The Advanced Mobile Access

The RAN part of our NMN architecture is the AMA. We anticipate the AMA to be based on 4G/5G cellular systems, standardized by 3GPP. AMA has two main characteristics: 5 Gb/s or higher access speeds and smaller cell sizes. Both of these will affect the requirements posed to the core network. AMA has its own control and management plane in the form of non-access stratum (NAS) signaling, radio resource control (RRC) layer, and so on, and an in-house operation and management (O&M) system.

The Optical Mobile Network

The core network in the NMN is the OMN, built on optical transport technologies. The increase in wireless access bit rate, and the availability of femto- and picocells and other portable base transceiver stations (BTSs) will increase the number of RAN devices that must be connected to the core in a given country. Taking Japan as an example, 100,000 BTSs during NMN deployment is a conservative estimate. Operators must take into account this high number of BTSs and their capacity when they dimension their transport network. By 2020, we estimate the need of a core network capable of sustaining a petabit-per-second class of traffic. This traffic will be generated by applications like video or live location-based services, and boosted by higher user consumption, encouraged by flat-rate billing plans and newer mobile terminals.

In order to transport such high traffic, we can only see optical switching and transport as a potential candidate for the future. High traffic brings two constraints in the core network: the total necessary bandwidth, and the energy consumption of the present power-hungry electrical routers. Optical switching and transport technology can solve these two problems simultaneously [7]. In this regard, passive optical networks (PONs) are suitable for connecting numerous BTSs in a cheaper but more bandwidth-efficient way. Generalized multiprotocol label switching (GMPLS) [8] is a good candidate for the control and management in an optical transport network.

However, optical technologies are less flexible than their electrical counterparts, when it comes to intelligent and dynamic routing decisions (e.g., during path failure). This is due to the fact that optical switching, such as variants of wavelength-division multiplexing (WDM), are done in the physical layer in λ units. One way of addressing this is to mix electrical switches with optical ones, where the electrical switches act as

Advantages	Challenges
Risk share with vendors	Need taller towers
Reduce CAPEX/OPEX	May limit competition
Improve bottom line	Can be used to undermine smaller competitors
Improve network quality	Needs new advanced sharing tools
Manage resources effectively	Needs detailed ground work
Improve cash flow	Needs organizational changes
New opportunities to increase revenue for incumbents	Interworking challenges
Source of cost efficiency	Needs third party vendors
Improve business focus	Risk of losing control. Initial costs in setting up the network sharing solution

Table 2. *Advantages and challenges of network sharing solutions.*

cluster heads. This will provide a regional flexibility in the otherwise rigid transport network. The O&M system can then instruct the electrical cluster heads to manage their surroundings in the desired way.

Other challenges arise from the fact that optical switching and transport is most efficient when traffic aggregation is maximum. This is a difficult criterion for a mobile operator, as mobile traffic is highly localized and dynamic due to user mobility. Smaller cell sizes increase handover further, and user traffic has to be frequently and dynamically de-aggregated to track the mobile user. With this respect, the placement of traffic aggregators becomes a planning problem that must take user mobility into account. Too much dynamicity will not be possible due to the inherent inflexibility in optical switches (e.g., the unavailability of optical logical units).

The Service Delivery Network

The SDN is the service platform for the future. Unlike conventional service development, where thousands of lines of codes need to be manually written over a period of months if not years, the SDN will provide service enablers [9] as ready-to-use service components. Here, the key point is the composition of multiple enablers to form or enrich a service. As distributed service components, in the form of enablers, have to interact with each other to make a meaningful service, we call this service platform itself a network. At present, SDN type entities do not come with a standardized or well-known control protocol. However, Rich Communication Suite (RCS) [9] or IMS can evolve as a control and management framework for such a platform.

Requirements for NMN Sharing Solutions

The huge cost of deploying an NMN, described above, will make network sharing solutions even more appealing in the future. Besides the requirements imposed on current network sharing solutions, enhanced future solutions shall also fulfill the evolved requirements of future mobile operators. The following requirements are derived from mobile traffic trends, service predictions, and mobile technology directions.

Requirements for industrial hosting: First, we briefly discuss the industrial requirements (carrier-grade) for network sharing among operators. High reliability and high quality are two of the most important factors influencing the successful operation of network operators. The isolation property of virtualization will guarantee network service quality by separating the coexisting networks' operations, thus reducing interference among services. Additional scaling/failover techniques can also provide higher reliability. Similarly, fast response time and low delay for in-network processing of the transported data flows and control messages are important requirements. Link virtualization for providing end-to-end transmission links, and centralized/distributed/hierarchal processing services enabled by server virtualization are some of the features that may fulfill these requirements. Last, the security/privacy level among the sharing network operators must be taken into account. The overall system should provide no opportunity for information leaks or control takeover by another operator, and should ensure the privacy protection of the individual operations. Inherently, virtualization technologies can satisfy these features.

Extended network sharing scope: Current network sharing solutions as summarized earlier mainly function within the scope of the access network. Their primary benefit is CAPEX and OPEX savings for the mobile operators, with additional efficiency gains in spectrum resource utilization in some cases. In this respect they are suitable for rural areas with low population density, where the revenue for network services is lower. Technically, these solutions function by means of pooling and splitting the spectrum resources, regulated through fixed service level agreements (SLAs) and roaming agreements. To the best of our knowledge, no solution currently exists for splitting of the whole end-to-end mobile network. At the same time, we are unaware of any solution that offers dynamic and flexible sharing of the infrastructure among operators, on timescales smaller than the current times needed for contract agreement and implementation (currently on the order of months or years). NMN architecture should address these limitations as a higher degree of sharing results in more cost saving.

Full isolation for data and control plane among virtual network operators: While the data plane in network sharing solutions can mostly be isolated among the operators involved through the use of separate data bearers defined in 3GPP specifications, the control and management plane of the common network infrastructure mostly remains common and accessible to all players. As a first consequence of this fact, the involved network operators have access to the same pool of control messages and can influence the functioning of the network (e.g., usage of sensitive network resources and customer information). In this respect, a full isolation of the operation of the different parties remains impossible. As a secondary consequence, the security and privacy of one operator's customers cannot be guaranteed and protected from the sharing, possibly malicious, operators. Third party solutions are developed in order to address these shortcomings, in which the maintenance and operation of the network infrastructure is outsourced to a trusted party. While this approach can solve the previously mentioned limitations, depending on the signed agreements with the third party management entity, it might defeat the original purpose of the network sharing idea (i.e., to cut costs for the operators). The requirement is to achieve full isolation in both the data and control planes, and inherently ensure full security and privacy among virtual network operators.

Possibility for virtual network customization: Current network sharing solutions offer limited options to mobile operators, and especially greenfield operators, in terms of functional optimization for specific deployed services. As there is no pure concept of data and control plane isolation among the operators sharing the infrastructure, the entities involved are forced to use the same communication and control protocols. However, operators desiring to use the network infrastructure in order to deliver specialized services to mobile clients might prefer the use of special transmission protocols, developed particularly for the targeted services. An example of such a scenario is a video service provider who wants to offer a multimedia streaming service for mobile clients. The current TCP/IP protocol stack, while still functional, is not optimized for video delivery, and additional/replacement protocols could be used for better performance (e.g., UDP, RSVP, SCTP). Currently, such an option is unavailable. The latest technologies (e.g., node and network virtualization), which enable full separation between entities sharing the same infrastructure equipment and hence allow for protocol stack differentiation among the players, are not leveraged in current network sharing solutions. Our architecture should leverage on current technologies in order to allow for full virtual network customization.

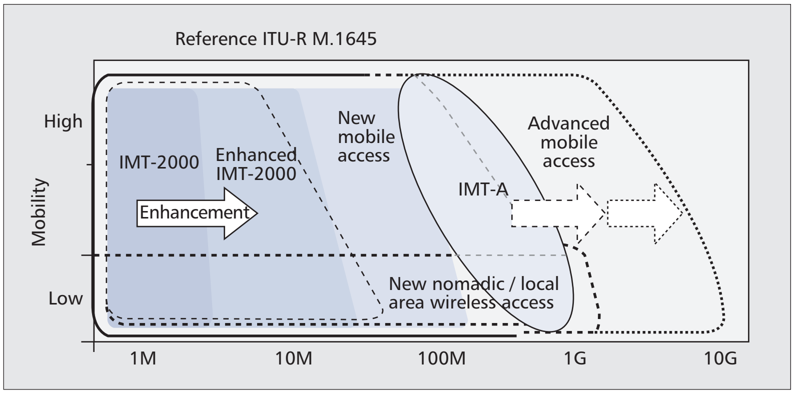


Figure 3. *ITU wireless access speed prediction.*

Combined control plane for end-to-end network sharing: The three main planes of NMN, as described earlier, come with separate control and management planes. Besides, the 3GPP network elements (e.g., xGSN/AGW) have their own control and management functionality [2]. At present, separate in-house O&M systems operate and manage these entities, and tasks are delegated to multiple departments within an operator. No single (i.e., integrated) O&M system exists that can holistically do resource control and management on an end-to-end basis (i.e., from the RAN to the application servers). As our objective is to facilitate network sharing over all the network planes, these separate O&M systems must be integrated/unified. Therefore, we require a mediator between the above-mentioned physical infrastructure and service providers, such as virtual network (VNET) operators who share the physical infrastructure. The proposed mediator, named the network configuration platform (NCP), is the most novel architectural building block for future network sharing solutions and is explained below.

THE NETWORK CONFIGURATION PLATFORM: INTEGRATED O&M FOR NETWORK SHARING

OVERVIEW

We introduce NCP to decouple the physical infrastructure (AMA, OMN, and SDN) from the users of the infrastructure. As multiple operators will share the infrastructure, we consider this decoupling indispensable. The first responsibility as well as novelty of NCP is the consolidation of the three control and managements planes of AMA, OMN, and SDN so that end-to-end resource management can become possible and by a single entity. It holds interfaces (I/Fs) with each control plane in the physical infrastructure (PHY). NCP will not directly do link management or server migration, but will ask the respective control planes (e.g., GMPLS or RAN O&M) to reserve resources at a coarser granularity. The granularity of such resource management and control, and its consequent administration within NCP (PHY topology database [DB] in Fig. 4) is

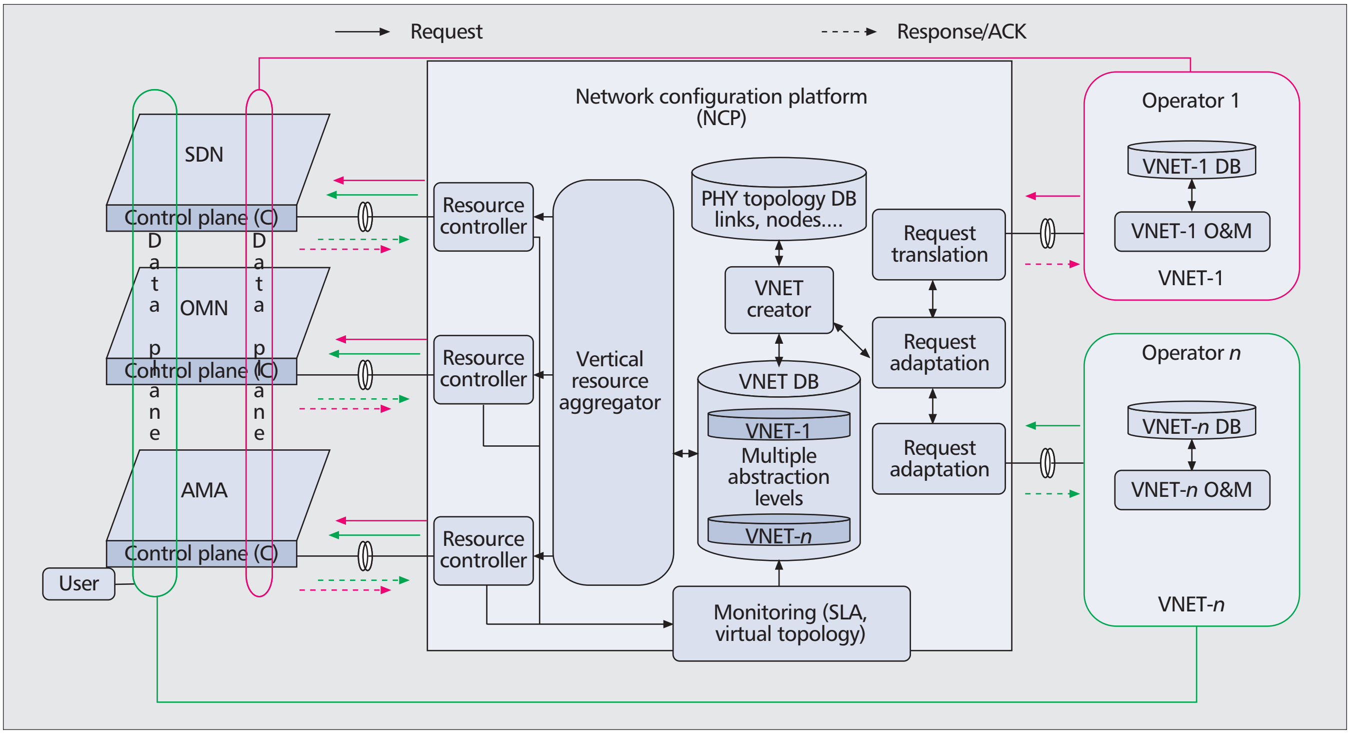


Figure 4. *General NMN architecture and integrated network configuration platform.*

an open issue. Our vision is that the resources in the physical network are virtualized, and NCP holds the information on the virtualized level and does the administration of this abstraction. The finest granularity would be every physical link, switch, and node being visible to NCP, and the administration being executed at this level. A coarser abstraction level could be an MPLS virtual circuit (VC), and IP routers that are the endpoints of the VCs, and end hosts. There is no difference between the PHY control planes and NCP in the former case. In the latter case, physical network control planes take care of each physical entity, whereas NCP administers only the coarser abstraction level visible to it. The different abstraction levels affect the scalability of NCP and must be determined not only by technical optimization results but also by business cases and usage scenarios. For example, an MVNO may only want to see the mobile terminals and application servers. Another operator who developed a proprietary routing protocol may want to see the routers/switches as well. A mobile operator planning to deploy a new generation of cellular technology would want to see the 3GPP network elements and RAN. The VNET creator generates such abstraction levels, and they are stored in VNET DB (Fig. 4).

NCP can provide a virtual network to a VNET operator in two ways: upon request from the operator or by its own advertisement. In the former case, NCP receives resource reservation requests from the operator; specifically, from the VNET O&M in each operator. A request translation and adaptation is necessary based on available resources in the PHY DB, and the VNET creator generates an image of the virtual network and stores it in the VNET DB. However, when the NCP advertises a different VNET as a service, it holds multiple abstraction levels for the physical resources and advertises them to the interested parties. VNET operators can choose a specific abstraction level that suits their purpose and ask NCP for reservation. One uniform resource description language (RDL) needs to be developed (many exist already but need functional completeness and standardization), through which VNET operators submit their resource requirements and SLAs to NCP.

Based on the abstraction level in the VNET DB, a virtual resource aggregator module computes physical resources necessary in the AMA, OMN, and SDN. As these are controlled and managed by separate control planes, respective resource controllers are informed by the virtual resource aggregator on what has to be reserved and the monitoring principles for the reservation. Resource controllers interact with the respective control plane to execute the resource reservation.

After resources have been duly reserved (i.e., an end-to-end virtual network has been formed), access to the resources is handed over to the VNET operator. The VNET operator holds the information about the part of the network it has rented in its VNET DB. The VNET operator controls and manages its share by its own O&M (e.g., quality of service [QoS] control), and NCP does not intervene unless asked. Monitoring and operation for SLA maintenance is an important issue here and is addressed later.

INTERFACES

Three general I/Fs between the architecture components are necessary and have to be standardized for vendor-independent deployment. These are briefly explained below.

I/F between PHY domains and NCP: The I/F is needed so that NCP can unify the separate control planes, issue resource reservation requests to the infrastructure, and perform dedicated monitoring and management. Extensions of the physical infrastructure control protocols will pass resource availability, reservation, and network health information to NCP. NCP will convey reservation requests, monitoring commands through this I/F. Such resource control and monitoring commands will be sent separately to separate network domains. The consolidation of resources over all three domains (i.e., SDN, OMN, and AMA) is NCP's responsibility, and the respective domains remain unaware of the other domains from the control point of view.

I/F between NCP and VNET O&M: The I/F is used to convey network requirements from the VNET operators to NCP, and to advertise virtual resources from NCP toward potential VNET operators.

I/F between the VNET operator and the PHY domains: This I/F is used by a VNET operator to access the parts of the network domain that are allocated by NCP in the form of a VNET. Network software installation, service performance, and data plane monitoring are performed through this I/F. Each I/F could include more than one functional interface.

Detailed specification of the I/Fs are an open issue and have to be determined among operators, vendors, and other role players.

Monitoring and Operation

As isolation by virtualization is the enabling technology for network sharing, some new problems arise in the operation of the whole architecture.

The physical infrastructure is controlled and managed by its own control protocol and is not visible to NCP in all its details. A VNET operator also cannot see the bare physical infrastructure. On the other hand, neither NCP nor the physical infrastructure can see inside a VNET operator's resources and its data plane. However, this separation in network control and management makes SLA violation difficult to detect, or at least delays the process. A data path inside a VNET operator can be affected by failure in physical infrastructure (e.g., link breaks due to cable cut off or a server shut down because of hardware malfunctioning). NCP can only know it if it is performing resource management at that abstraction level. However, a VNET operator cannot see it as it does not have access to physical devices and transmission lines. It only sees its data path is broken or an application server is down. It will start a system health check and has to be sure that the faults are not due to problems in its routing protocol or application software or any resources it brought into its share. Only then can it report to NCP that there is an SLA violation, and NCP will ask the PHY control plane to detect the cause of the failure. This is an open issue and needs serious investigation. The isolation by virtualization envisioned in the research community may not be easy to achieve for the reason explained above.

Enabling Technologies

There are several methods available for link virtualization. Some potential candidates are λ-level layer 1 (L1) virtual private networking (VPN) and layer 2/2.5/3 (L2/L2.5/L3) tunneling [8]. All these levels can be holistically managed by GMPLS, which is a good candidate to generate multiple levels of link/path abstraction necessary in NCP. However, GMPLS cannot run multiple networks at the same time and needs extensions. OpenFlow and Flow Visors can also virtualize links/paths at the flow level [10], and are good candidates for OMN virtualization where the management node can sit in NCP.

For nodes such as application servers and 3GPP network elements, well established host virtualization technologies can be deployed, as we have seen in the Amazon EC2 cloud [11]. However, so far these concepts have not been used in a nationwide, integrated network virtualization scenario, where virtual networks must be fully isolated. Isolation, scalability, and ease of control and management aspects have to be investigated in order to utilize such methods in network virtualization and the consequent reconfiguration of such networks to ensure six 9s commercial operator networks.

Isolation, scalability, and ease of control and management aspects have to be investigated in order to utilize such methods in network virtualization and the consequent reconfiguration of such networks to ensure six 9s commercial operator networks.

Discussion and Open Problems

The proposed new architecture for network sharing based on virtualization technologies is expected to address the limitations of current sharing solutions. However, in order to transform this architecture into a viable cost-effective platform, some open issues remain.

The depth of virtualization: Virtualization technologies can be applied at different levels of the protocol stack for the network links, and at different levels of the machine architecture for the network nodes and servers. Virtualization at each level is characterized by certain features, performance metrics, and cost of implementation and maintenance. Furthermore, it influences the level of functionality transfer from the infrastructure providers to the VNET operators. A careful trade-off of all these issues must be considered when deriving a full end-to-end solution for network sharing.

Interface implementation: As mentioned before, three different types of interfaces are required in order to realize our proposed architecture. While for the implementation of some of these interfaces communication protocols already exist, some new protocols must be derived. Especially, the representation, request, and reservation of virtual resources (e.g., through means of a resource description language) at different abstraction levels must be standardized to facilitate the implementation of the interfaces between virtual network controllers, NCP, and physical network domains.

The unified control plane: One of the largest tasks of the NCP is to unify the control of the different physical network domains. This will be a challenging task, as currently each network domain operates under its own control protocol, which is, moreover, technology-dependent. Finding the right abstraction for each control plane, defining the interactions among these planes, and deciding the extent to which the NCP takes over the individual control planes is a large research issue.

Inter-VNET-operator mobility management: As the VNET operators in our proposed archi-

Realizing NMN in a nationwide commercial networking context is a formidable task and many open issues need to be addressed. No single player can answer all the issues and collaboration among academia, vendors and operators is indispensable to realize such futuristic, highly functional, value-added networks.

tecture get access to physical network resources in an isolated way, their handling of user services and user management will also be separated. With this respect the roaming of users among different VNET operators must be addressed by a new paradigm, which takes into account the new features of the proposed architecture. This scenario in the mobile network is analogous to the inter-VNET interaction case for fixed networks.

Cost of virtualization: Decoupling the control and management from physical network operation and physical network usage through virtualization reduces the control and management complexity in each player (i.e., VNET operator, NCP, and PHY). However, new building blocks like NCP, and additional technical components like network-wide hypervisors,and extensions of PHY control protocols, will increase CAPEX compared to the available network sharing solutions explained earlier. The servicing cost for the end users (e.g., a mobile phone subscriber) will be determined by the total cost (i.e., TCO of PHY, NCP, and VNET operators added together). In the highly competitive mobile market, end users' subscription fees must not rise without valid justification. Virtualization brings new qualitative dimensions in network sharing and the consequent operation. However, the cost analysis of such a scenario is highly important, as no operator will follow such a business scenario unless its cost effectiveness is proven.

Conclusion

In this article, we propose a next mobile network architecture with emphasis on network sharing for reduced TCO. The shortcomings of available sharing technologies have been vividly explained, and virtualization has been proposed to overcome such shortcomings. As virtualization increases O&M complexity, the mediator entity NCP was introduced in order to decouple the O&M of running a physical infrastructure, slicing the infrastructure to create virtual end-to-end networks, and operating such virtual networks. We do not restrict our architecture to sharing only among mobile operators, but also with fixed network operators by segmenting the network into three functional planes. There are many enabling technologies available today that will be handy in realizing such a virtualized network. However, realizing NMN in a nationwide commercial networking context is a formidable task, and many open issues, mentioned in this article, need to be addressed. No single player can answer all the issues, and collaboration among academia, vendors, and operators is indispensable to realize such futuristic, highly functional, value-added networks.

Acknowledgement

We thank Dan Jurca, presently with Huawei Technologies, for his contribution to and comments on this article, and his work on NCP architecture development during his tenure at DOCOMO Communications Laboratories Europe GmbH.

Part of this work has been funded by the German Federal Ministry of Education and Research under grant number 01BK0916.

References

[1] Cisco Visual Networking Index: Global Mobile Data, Traffic Forecast Update, 2009-2014, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white paper c11-520862.pdf.

[2] 3GPP TS 23.251 V2.0.0 (2004-6), "Network Sharing; Architecture and functional Description," Rel. 6, June 2004.

[3] C. Beckman and G. Smith, "Shared Networks: Making Wireless Communication Affordable," *IEEE Wireless Commun.*, Apr. 2005, pp. 78–85.

[4] Mobile Network Sharing Report 2010-2015 — Development, Analysis & Forecasts, Market Study, Visiongain, Mar. 2010.

[5] T. Frisanco, P. Tafertshofer, and R. Ang, "Infrastructure Sharing for Mobile Network Operators," *Int'l. Conf. Info. Networking*, Jan. 2008, pp. 1–5.

[6] M. Yabusaki, Y. Okumura, and M. Tamura, "Next Mobile Network Architecture," *IEEE ICC '10*, Cape Town, South Africa, May 2010.

[7] M. Kakemizu and A. Chugo, "Approaches to Green Networks," *Fujitsu Sci. and Tech. J.*, vol. 45, no. 4, Oct. 2009, pp. 398–403.

[8] N. Yamanaka, K. Shiomoto, and E. Oki, *GMPLS Technologies: Broadband Backbone Networks and Systems*, CRC Press, Taylor & Francis Group, 2006.

[9] Rich Communication Suite (RCS), GSM World, http://gsmworld.com/ourwork/mobilelifestyle/rcs/index.htm

[10] N. McKeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 38, issue 2, Apr. 2008, pp. 69–74.

[11] Amazon EC2, http://aws.amazon.com/ec2/.

Biographies

Ashiq Khan (khan@docomolab-euro.com) received his B.E. and M.E. degrees from Tohoku University in 2002 and 2004, respectively. He joined the Networking Research Laboratories of NTT DOCOMO, INC. Tokyo, Japan as a research engineer in 2004 and worked on autonomous mobile networks, QoS-based routing algorithms, future service delivery platforms and next generation network architecture. He is a senior researcher now at DOCOMO Communications Laboratories Europe GmbH, Munich, Germany. His research interests include future mobile network architecture, network virtualization, and control and management of 4G and beyond cellular networks.

Wolfgang Kellerer (kellerer@docomolab-euro.com) is the director and head of the Network Research department at NTT DOCOMO's European research laboratories in Munich, Germany. His research interests include mobile networking, QoE-based resource management, service platforms, and overlay networks. Before he joined DOCOMO Euro-Labs, he was a research staff member at Munich University of Technology (TUM). In 2001 he was a visiting researcher at the Information Systems Laboratory of Stanford University, California. He holds an M.Sc. and a doctoral degree in electrical engineering and information technology from TUM, Germany.

Kazuyuki Kozu (kozu@docomolab-euro.com) is a research manager at DOCOMO Communications Laboratories Europe GmbH. He received his B.E. and M.E. degrees from Yokohama National University in 1995 and 1997, respectively. He joined NTT DOCOMO in 1997. He has worked for NTT DOCOMO in the area of mobile core networks. His research and development activities covered designing mobile network architecture and 3GPP standardization. Since 2010, he is a member of DOCOMO Euro-Labs and is involved in research on next mobile networks.

Masami Yabusaki (yab@docomolab-euro.com) is the president and CEO of DOCOMO Communications Laboratories Europe GmbH. He received his B.S., M.S., and Ph.D. degrees from Waseda University in 1982, 1984, and 1993, respectively. He joined NTT in 1984. He was engaged in research of an SS-TDMA system, research, development and standardization of PDC, IMT-2000, and all-IP mobile networks. He is currently promoting research on next mobile network and network value-added services.