Network Virtualization: Opportunities and Challenges for Operators

EDIN 0593-1956
Project P1956
For full publication
December 2010
Authors

Jorge Carapinha, Portugal Telecom Inovação
Peter Feil, Deutsche Telekom AG
Paul Weissmann, Deutsche Telekom AG
Saemundur E. Thorsteinsson, Síminn hf.
Çağrı Etemoğlu, Türk Telekom A.S.
Ólafur Ingþórsson, Síminn hf.
Selami Çiftçi, Türk Telekom A.S
Márcio Melo, Portugal Telecom Inovação

Editor: Jorge Carapinha

Disclaimer
This document contains material, which is copyright of EURESCOM Study Programme Subscribers and may not be reproduced or copied without permission. The information contained in this document is the proprietary confidential information of certain EURESCOM Study Programme Participants and may not be disclosed except in accordance with Section 5 of the EURESCOM’s general conditions of the contract.
All Participants have agreed to the full publication of the report.
Neither the Participants nor EURESCOM warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

P1956 Network Virtualization – Opportunities and Challenges

2
Summary

- What is Network Virtualization
- Scenarios for Network Virtualization Uptake
- Opportunities for Operators
- Challenges Ahead
- Conclusions
Network Virtualization Attributes

- **Abstraction**
  - Details of the network hardware are hidden

- **Indirection**
  - Indirect access to network elements, network nodes may be combined to form different virtual network topologies.

- **Resource sharing**
  - Network elements can be partitioned and utilized by multiple virtual networks

- **Isolation**
  - Loose or strict isolation between virtual networks must be provided
Decoupling Networks from Infrastructure

Virtual Networks

Virtualised Substrate

Physical Infrastructure

Management of virtual networks

Provisioning of virtual networks

Virtualisation of resources

Collection of virtual resources, aggregated to build virtual networks

Infrastructure made of virtualizable network resources

Independent, isolated VNs, running different protocols, packet formats, management tools, etc.
NV as Catalyst for Network Evolution and Technology Pluralism

Legacy:
Infrastructure layer (roughly OSI layers 1-3) very simple; service layer has to be overburdened to compensate for rigidity of infrastructure layer

NV:
Virtualization “hides” the infrastructure and permits to tailor networks to service characteristics; makes service creation easier and more flexible
Network Virtualization: (R)Evolution

1980s – Link virtualization (ATM, FR virtual circuits)
1990s – Node Virtualization in the edge (MPLS VPNs)
2000s – Virtualization of IT resources
2010s – “Full-blown” Network Virtualization
At the physical level, NV enables mobility of network resources according to dynamic network conditions or service demand cycles. At the virtual network level, NV enables elasticity of the virtual resources.
Relevant Projects and Initiatives

- European Projects
  - 4WARD
  - FEDERICA
  - G-LAB
  - AGAVE
- North-American Projects
  - CABO
  - GENI
  - OpenFlow
  - UCLP
- Asian Projects
  - Akari
  - NVLAB
- Other Projects
  - PlanetLab
Roles and Players

- **InP** owns, controls and administers physical resources, which may be used, or offered to 3rd parties, to build custom-tailored VNs.
- **VNP** assembles a VN, according to a given description and based on resources from one or more InPs.
- **VNO** establishes, manages and operates VNs; handles end user attachment.
- **SP** provides services to end users; NV is supposed to be invisible from the SP perspective.
- **End user** is the user of the service offered by the SP (or directly by the VNO if a distinct SP does not exist as such).
Scenarios for Network Virtualization (1) Network as a Service (NaaS)

- Clear separation of the roles of the InP and the VNO

- Value for Operators
  - New revenues for the InPs
  - Lower CAPEX/OPEX for VNOs compared to building a network based on physical resources

- Optionally, the VNP plays a VNO/InP mediation role to locate and aggregate the virtual resources that compose a VN (likely to be the case where a VN spans multiple InP domains). Possible deployment scenarios:
Gaps and Open Issues for NaaS Scenario

- It’s impossible to find a unique model to describe inter-relationships between network virtualization players.

- It is not clear whether virtual networks would be as reliable as non-virtual ones.

- Standardization efforts are not mature yet to enable interoperability between heterogeneous domains.

- As compared to existing technologies (MPLS VPNs), an approach to provide a stricter isolation of link resources is needed.
Isolation provided by NV enables technological heterogeneity and diversity in the same network infrastructure.

Value for Operators:
- Coexistence of production and experimental networks – experimentation of new technologies in real environment
- Coexistence of legacy and new technologies – easy technology migration
Gaps and Open Issues for Experimentation and Migration Scenario

- Isolation for both security and resource allocation needs to be proven in real-world scenarios.

- A political consensus is needed between all divisions in the company to allow use of VNs for experimentation on production infrastructure.

- The “real-world data” requirement of VNs used for experimentation conflicts with the isolation requirements of the remaining network.

- How OPEX would be affected by running several concurrent VNs with different technologies is a question mark.

- How a new successful networking technology would be integrated to the VN system is an open issue.
Scenarios for Network Virtualization (3) Network Partitioning in Service-Specific VNs

- NV enables convergence of disparate services (e.g. Internet, voice, IPTV, business services) over a common infrastructure providing each service with a network tailored to its characteristics.

- NV enables network elasticity: networks can be made smaller or larger on demand, according to needs.

- Value for Operators:
  - Possibility to achieve service convergence without a “1-size-fits-all” solution
  - Coexistence of legacy and new technologies – easy technology migration
Dealing with the increasing number of services as well as increasing number of subscribers for each service would be challenging.

How Telco services such as TV and Telephony would be integrated with the related applications hosted inside operators’ clouds is an open issue.

How this scenario could be realized in cases where more than one Telco acting as InP for a VN needs to be clarified.

The level of isolation needs to be determined based on the business model and service type.
Scenarios for Network Virtualization (4) Cloud Computing and CDNs

- Coordinated control of IT and network resources (which can now be viewed as a single collection of virtualized, dynamically provisioned resources)

- Value for Operators:
  - Providing options for VNOs to offer customized cloud networking solutions for individual customers or customer segments
  - Providing premium distribution of content from origin servers and/or replication servers to the relevant ISPs
Gaps and Open Issues for CC&CDN Scenarios

- Limitations of supporting distributed cloud service provisioning, i.e. the virtual networking assumes a static end-to-end connection.

- Seamless networking handover technologies are still immature and inefficient for CC case.

- Potentially complex service delivery process or business models for CC.

- Is it possible or beneficial/economical to extend a VN to multiple replication servers for optimum content delivery to the end-user?

- The required virtualization capabilities of load balancers in CDNs are still being developed.

- The business case is unclear for CDN networks.
Opportunities for Operators (1)

- Enabling new business models for the existing and the upcoming services
- Offering a new role in network architecture for the existing and the new operators: Virtual Network Providers
- Ease of network and service provisioning due to NV’s flexible nature
- Enabling Telcos to offer a wide variety of Quality of Service levels for each service.
- Allowing operators to adapt quickly to service demand variations and market dynamics
Opportunities for Operators (2)

- Possible CAPEX/OPEX reduction for the existing operators
- Accelerating the market entry of new vendors due to NV’s lower CAPEX requirement for VNOs and VNPs on hardware
- Increase vendor independence in operators’ networks and data centers
- Creating an environment for innovation in operators’ networks and adoption of disruptive technologies without interfering with legacy traffic and services, or affecting existing business
- Offering economical solutions to the ongoing process of large-scale rollout of fiber closer to customers (e.g. FTTH/FTTC).
### Challenges to Deploy Network Virtualization

<table>
<thead>
<tr>
<th></th>
<th>Network as a Service</th>
<th>Experimentation and Technology Migration</th>
<th>Network partitioning</th>
<th>Cloud computing/CDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier-grade reliability</td>
<td>***</td>
<td>***</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td>Scalability</td>
<td>***</td>
<td>*</td>
<td></td>
<td>**</td>
</tr>
<tr>
<td>Isolation</td>
<td>***</td>
<td>**</td>
<td>**</td>
<td>***</td>
</tr>
<tr>
<td>Interoperability</td>
<td>***</td>
<td>***</td>
<td></td>
<td>**</td>
</tr>
<tr>
<td>Security</td>
<td>***</td>
<td>***</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td>Operational complexity</td>
<td>***</td>
<td>*</td>
<td></td>
<td>***</td>
</tr>
<tr>
<td>Quality management</td>
<td>***</td>
<td>***</td>
<td>**</td>
<td>***</td>
</tr>
<tr>
<td>Programmability</td>
<td>*</td>
<td>***</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Accountability</td>
<td>***</td>
<td>-</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Monetization</td>
<td>***</td>
<td>-</td>
<td></td>
<td>**</td>
</tr>
</tbody>
</table>

*** Crucial challenge; will surely represent an obstacle if an appropriate solution cannot be found.
** Major challenge; may represent an obstacle to widespread deployment.
* Minor challenge; should be addressed, but does not represent a major obstacle in this specific use case.
- Not relevant in the scope of this specific use case.
Possible Threats to Operators due to NV

- Today’s Telco-MVNO relationship can be seen as an example for future InP-VNO/VNP relationship.

- NV would be a threat to the operators to act as InP due to
  - low margins posed by regulatory interventions,
  - possible competition between InPs to offer infrastructure to VNO/VNP, and
  - the investment risk for building up the infrastructure.

- NV would be a threat to innovative VNO and to the whole business environment because innovation would be hindered.
  - Innovative VNO would like to implement his ideas to increase his business.
  - InP is very unlikely that the InP would be willing to invest in the upgrade due to lack of investment return.
  - In cases where many VNOs other than the innovative one are customers of the same InP, other VNOs would oppose the upgrade due to possible price increase.
Areas for Standardization

- VNP/InP interface: A standard resource description language is required to describe networks and network resources.

- InP/Network equipment interface: Standards will facilitate the InP’s management of physical resources and fasten the setup of virtual nodes and links.

- InP/InP interface: It is used to setup virtual links and networks spanning multiple network infrastructure domains, including the case where two InP are indirectly connected, i.e. through non-virtualized network domains.

- Signaling for virtual link / virtual node setup: Standardization is required to enable automated establishment of virtual networks.

- Security and resource isolation: It is required to prevent or mitigate the impact of DoS attacks or misconfiguration in neighboring virtual networks.
Interfaces and Standardization

1. VNO/VNP: Virtual network description and request
2. VNP/InP: Request and negotiation of virtual resources
3. InP/Network elements: Setup of virtual nodes and virtual links
5. VNO/InP: Virtual node access for bootstrapping
6. End user/VNO: End user attachment

P1956 Network Virtualization – Opportunities and Challenges 24
Conclusions and Final Recommendations (1)

- Network virtualization has been successfully demonstrated in small-scale research testbeds, but it is clear that there is still a way to go before it can be considered mature for large-scale commercial deployment and carrier-grade reliability is guaranteed.

- Network virtualization decouples networks from infrastructure – this enables:
  - Flexible “on-demand” setup and reconfiguration of networks;
  - Coordinated control of IT and network resources (which can now be viewed as a single collection of virtualized, dynamically provisioned resources)

- Network virtualization offers advantages in several contexts and can be exploited in multiple scenarios:
  - Enabling new business models – e.g. Network as a Service;
  - Partitioning of the infrastructure in customized service-specific virtual networks;
  - Experimentation and migration to new technologies and services.
  - Cloud computing and CDNs
Conclusions and Final Recommendations (2)

- Deployment in ‘carrier-grade’ commercial environments still faces multiple challenges:
  - Features like reliability, scalability, isolation, security demand further attention.
  - Commercial scenarios like NaaS may not be feasible in the foreseeable future.
- Standardization, still in an early stage, will be key to enable interoperability and avoid vendor lock-in.
- Other emergent trends, e.g. cloud computing, must be put in perspective, in order to exploit synergies.
- Relevant industry activities, namely OpenFlow, supported by major vendors (e.g. Cisco, NEC) must be followed closely by operators.