SLICING WITH NON-PUBLIC NETWORKS

An other orchestration challenges for the next decade

Jose Ordonez-Lucena, Telefónica I+D
Lisbon, 27th November 2019

This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 856709
Exploring the future: public and non-public networks

- Vertical use cases may involve the combination of public networks and NPNs.

- The MNO may need to provide network **resources, functions and services** to industry verticals
  - From the public network
  - In a cost-effective manner

- Network Slice as-a-service (NSaaS) as a future-proof service delivery model, with the NSI...
  - provided by the MNO
  - consisting of network functions hosted by the public network
The gist of NSaaS: slice capability exposure

- Two complementary service views in NSaaS:
  - Resource-facing view (NSI deployment details) VS Customer-facing view (NSI exposed capabilities)
  - Abstraction to preserve the required demarcation point between the MNO and the industry vertical

- A vertical could want to retain some control over the NSI provided (as a service) by the MNO
  - Getting involved beyond passive monitoring
  - Operational coordination with the service components deployed on the NPN.

- Tailored customer-facing view of the NSI -> slice capability exposure
  - Allows the MNO to grant an industry vertical with necessary control capabilities over the NSI
Reference architectural framework in NSaaS
NSaaS phases

- Two main phases

**Network Slice (aaS) Request**

The NSaaS customer issues a service order towards NSaaS provider, requesting the deployment of a tailored network slice.

**Network Slice (aaS) Operation**

The NSaaS customer monitors and takes (some) control over the network slice, deployed and made available by the NSaaS provider.

- Slice Topology
- Slice Requirements
- Slice performance assurance and fault supervision
- Slice Management & Control
Network Slice (aaS) operation – Exposure levels

- In NSaaS scenarios, different verticals may want to take a more or less proactive role in the operation of their slices.
- Exposure levels -> levels of control the vertical can take over the provided slice.

<table>
<thead>
<tr>
<th>Customer is able to consume operations related to...</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E2E network slice</strong> application layer config &amp; management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Network slice subnet (and NF)</strong> application layer config &amp; management -&gt; 3GPP scope for RAN and CN, IETF scope for TN.</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Network slice subnet (and NF)</strong> virtualized resource layer config &amp; management -&gt; ETSI NFV network service (and VNF) orchestration</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Resource</strong> control and management at the virtual infrastructure layer -&gt; NFVI with optional EPA capabilities and infrastructural SDN control</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
Network Slice (aaS) operation – Exposure levels

- Token-based authentication

---

**NSaaS Provider Admin Domain**

REST API (programmability)

**E2E Network & Service Mgmt Functions** (include NSMF)

- **Virtualized Mgmt Domain**
  - NFVO
  - VIMs

- **RAN Mgmt Domain**
  - RAN Mgmt Functions
    - (include RAN-NSSMF + RAN-NFMFs)

- **TN Mgmt Domain**
  - TN Mgmt Functions
    - (include WiM + IP/Opt/ MW SDN controllers)

- **CN Mgmt Domain**
  - CN Mgmt Functions
    - (include CN-NSMF + CN-NFMFs)

**Provider’s Network (Public Network)**

**UE CPE**

**NSaaS Customer Admin Domain**

**Industry Vertical’s Management System**

**Customer’s Network (NPN)**

---

**UE CPE**
The Challenges Ahead - A Matter of Balance

• Integrated support for management and orchestration
  ➣ At all segments and all technologies
  ➣ Towards full network programmability

• Open full accountability
  ➣ Non-repudiation and auditability
  ➣ Means for assurance and SLA verification

• Predictive orchestration
  ➣ Aiding seemingly infinite capacity and zero perceived latency

• User requirements and operational policies
  ➣ Intent dialectics and elastic policy enforcement
  ➣ Compositional mechanisms for requests in multi-tenant environments

• Sensing and acting
  ➣ Open and extensible mechanisms for data and action streams
  ➣ Apply and manage (meta-)data about the network to improve orchestration
  ➣ Converged control action representations
This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 856709

Telefonica