SDN-NFV: An introduction

Telefónica I+D @ Global CTO
30.10.2014
We are evolving towards a **Hyper Connected and Intelligent Digital World**

*The explosion of digital services makes connectivity services more needed than ever*

**Smartphone is changing everything**

- **Reduction of Time to Market**
- **Radical increase of traffic** in telco networks
- **New ways of communication** and increasing number of “always-on” users
- **But the phone service continues to be the only universal service**...

(*) César Alierta, TEF CEO. TEF Digital Investor’s Day 2012
This digital world is introducing relevant challenges for telecom operators...

- There is a significant shift in revenue streams (driven by the expansion of internet).
- Telco expenditures and investments grow higher than revenues.
- New and legacy technologies are piling on top of each other.
- Operation complexity grows consequently.
- Uncertainty
- Complexity
- Unsustainability

Impossibility of predicting the new Internet Killer Application and how it will impact in the network.

But it is highly probable that it is associated to new devices.
Beyond evolution: evolution is mandatory to keep in the market. Transformation is the only way to lead...

Network evolution is reasonably under control…

...from 3G to 4G
...from copper to fibre

The challenge is transforming the network and its operation taking into account the inertia of its legacy
What are the current limitations of Telco’s networks?

Long innovation cycles (2-6 years)

- Long standardization cycles
- Scale is needed to introduce innovations

Complex Network Management

- Small changes in a network element requires an adaptation of the EMS (Element Management System)
- Complex stitching of network functions across segments and technologies, since network nodes are tightly coupled to the network segment and technology

Hardware and Software vertically integrated

- Capacity is tied to a function
- Vendors lock in (it is difficult to switch from one vendor to another when deployments are made)

Difficult IoT

- Interoperability tests required per protocol and node
We need to adapt and define the change to lead in the Digital era

**Telco players**
- Very intensive in hardware
- Capital intensive
- Software is not a core

**Internet players**
- Very intensive in software
- Can have global impact with not too much capital
- Hardware is a support, and is located in the network periphery
Components for this vision
Components for a “liquid network”
Or maybe by non-example

SDN BY EXAMPLE
IaaS in a data centre: per user requirements

- **Well-known design**
  - Chaining FWs to increase the level of protection
  - DMZ to place resources that need to be connected to the Internet with some level of protection
- **This is current best practice that is implemented on separate boxes nowadays**
- **Users expect to have the same level of protection when outsourcing this infrastructure to an IaaS provider**
The datacenter replicates the logical IaaS structure for every client...

... and this challenge has limitations with the current paradigm

Fine grained connectivity & isolation require extensive use of VLANs & firewall rules (and combine them!)

A large number of VLANs

Expensive equipment
“Client stitching”... or how to combine a VM server with a common networking infrastructure

- First solution
  - Provide virtualised FW functionality
  - Provide network isolation using VLANs
  - Provide isolated switching realms
- And this for each client...
- Since there is virtualisation and the system was controlled by a “software”, the vendor claimed this was SDN
The acronym war

S
Software

D
Driver
Defined

?  

N
Network
So... What is SOFTWARE DEFINED NETWORKING?

- Software Defined Networking is recognising that
  1. The network is not a shapeless entity AND network shape matters
  2. Network nodes don’t need a massive amount of intelligence for bringing packets from port A to port B
  3. Distributed is nice, but not a DOGMA
How do you SDN?
What are the implications?

• The data plane can be simplified
  • Best case scenario is using commercial off-the-shelf boxes
  • The x86 architecture
    • Is known to provide significant throughput
    • Provides a lot of interesting features to make the network flexible (virtualisation...)

• The control plane
  • Also benefits from the advances in the x86 architecture
  • Better control of the control plane features means
    • More overall stability
    • More flexibility, when wisely used
But this is complex, right?

- Of course... Did I ever say it would be easy
- However, the process is worth the gain
- A significant community has been working on this for the last couple of years
  - Network Operators
  - Hardware suppliers
  - Software suppliers
  - ...

ETSI NFV-ISG
NFV ISG vision & objectives...

NFV ISG vision:
“Leverage standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches, and storage”

Traditional Network Model

- DPI
- BRAS
- GGSN/SGSN
- PE Router
- Firewall
- CG-NAT
- Session Border Controller
- STB

NFV Model

- DPI
- BRAS
- CG-NAT
- GGSN/SGSN
- Firewall
- PE Router

VIRTUAL APPLIANCES

ORCHESTRATED, AUTOMATIC & REMOTE INSTALL

STANDARD HIGH VOLUME SERVERS
The ETSI NFV Reference Architecture
Bringing packets from A to B

SOLVING THE NETWORKING PART
Getting back to packet handling...

- Handling packets can be part of the headache
- However, virtualisation can help us getting rid of it
One candidate for packet handling can be OpenFlow:

- OF places packet handling logic into a centralised controller
- Easy to manage
- Some network functions become a program executed in the controller
- Smooth coordination between network and computing
- OpenFlow switch role can be played by the own hosts! (Open vSwitch)
OpenFlow in green-field deployments

- OpenFlow in the switching infrastructure
- OpenFlow integrated in the server
  - Open vSwitch is already built-in in the commonest virtualisation environments and the latest Linux kernels (3.3)
- Other SDN control protocols also applicable
... or in evolutionary scenarios, where legacy switching elements can be preserved

- Maximise reuse
  - Rely upon existing Layer2 or Layer3 connectivity
  - Use OVS in the servers only
- Nicira Networks’ approach
Network Function Virtualisation

CHALLENGES
Performance & Portability are required to fully accomplish NFV ISG objectives...

NFV ISG vision:

“Leverage standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches, and storage”

Traditional Network Model

- DPI
- BRAS
- GGSN/SGSN
- PE Router
- Firewall
- CG-NAT
- Session Border Controller
- STB

NFV Model

- DPI
- BRAS
- CG-NAT
- GGSN/SGSN
- Firewall
- PE Router

ORCHESTRATED, AUTOMATIC & REMOTE INSTALL

VIRTUAL APPLIANCES

STANDARD HIGH VOLUME SERVERS

TO FULLY REALISE THIS VISION:

Virtualised network appliances should provide high performance...

... while being portable between servers (& hypervisors)
... while providing the telco ecosystem actors a more predictable and manageable environment

VIRTUAL NETWORK FUNCTIONS PROVIDERS

Would not need to be aware beforehand of the infrastructure server on which their SW would be deployed in the end...

... but still can provide realistic performance estimations for different sets of HW (& hypervisor) setups.

HARDWARE (& HYPERVISOR) PROVIDERS

Could describe their equipment in objective terms, suitable for automated network operation.

Would not need to be aware beforehand of the virtual network functions which might be deployed in their servers.

NETWORK OPERATORS

Define a set of requirements for network functions to be deployed and their target performance.

Might be partially unaware of low-level details of each network function’s HW requirements: Provision & management can be uniform & automated.
MANO
NFV Orchestration Overview

L2/L3 Network Fabric Components & Network Connectivity Functions
- Switches*
- Routers
- Server NIC

Virtual Network Overlays
- vNIC
- vswitch

NOTES:
* includes OpenFlow Switches and Controllers
** It could be single Tier or Multi-Tier App

Network Functions
- Firewalls
- Load Balancer
- Traffic Steering
- NAT
- L4-L7 Routing
- WAN routers
- CDN
- EPC
- ...

VNF App

Non-VNF

Compute
- Servers
- VM

Storage
- Storage Arrays
- Local Storage
- SSD
- SAN
- NAS
- LUN

Network Functions
- Firewalls
- Load Balancer
- Traffic Steering
- NAT
- L4-L7 Routing
- WAN routers
- CDN
- EPC
- ...

BE MORE
DISCOVER, DISRUPT, DELIVER
Riding the liquid network
Components for a “liquid network”

- Software Defined Networking
- Network Function Virtualisation
- Open Innovation
What is the promise of Network Virtualisation?

It is an opportunity to build mouldable Networks and redefine the Architecture:

- Makes the infrastructure uniform
- Reduces IoT complexity
- Improves management of risk in a changing and ambiguous environment
- Introduces capacity in an easy and flexible way
- Fosters competition (new entrants) and innovation
- Prevents hardware scale from being an entry barrier

### Traditional Network Model: APPLIANCE APPROACH

- Network functionalities are based on specific HW with specific SW linked to HW vendors
- One physical node per role

### Virtualised Network Model: VIRTUAL APPLIANCE APPROACH

- When possible, network functionalities are **SW-based** over COTS HW
- Multiple roles over same HW

**Virtualised Network Model**

- ORCHESTRATED, AUTOMATIC & REMOTE INSTALL

**Function**
- DPI
- BRAS
- CG-NAT
- GGSN/SGSN

**Capacity**
- STANDAR DH AUGMENT SERVERS & SWITCHES

**Virtual Appliances**
- PE Router
- Firewall
A simple equation to define Network Virtualisation: \( NV = NFV + SDN \)

**NFV**
- **SW-defined network functions**
  - Separation of HW and SW
  - No vertical integration
    - HW vendor ≠ SW vendor ≠ Mgmt vendor
  - Once network elements are SW-based, HW can be managed as a pool of resources

**SDN**
- **Interconnecting Virtual Network Functions (a.k.a. backplane)**
  - Separation of control and data plane
  - Easy orchestration with SW domain
Network Virtualisation provides a mean to make the network more flexible, taking for granted a common HW layer.

Network functions are fully defined by SW, minimising dependence on HW constraints.
Network virtualisation helps reducing network management complexity, as HW can be treated as a pool of resources.

**APPLIANCE APPROACH**

- Node sizing is determined by the bottleneck of its functionalities.
- Capacity growth often leads to node growth or silo HW purchase.

**VIRTUAL APPLIANCE APPROACH**

- HW becomes interchangeable and aggregatable (pool).
- Resource assignment becomes fully flexible and dynamic.

**SESSION MGT LIMITATIONS PER NODE LEADING TO 2nd NODE PURCHASE**

**Vs.**

**PROCESSING CAPACITY BECOMES COMMODITY & MANAGED AS A CONTINUUM**

- Spare capacity for extra growth (in any functionality).
- Session MGT switching.
Software Defined Networking provides a first mean to improve operation and control of networks.

- **Network equipment as Black Boxes**
  - SDN
  - Open interfaces (OpenFlow) for instructing the boxes what to do

- **Boxes with autonomous behaviour**
  - SDN
  - Decisions are taken out of the box

- **Adapting OSS to manage Black Boxes**
  - SDN
  - Simpler OSS to manage the SDN controller
This new network model will help us to deeply transform our factory.

**Network Paradigm Change**

- **Computing principles** used in IT world are beginning to be applied in telecoms by the means of **Network Virtualization**
- **IP** as common language for **all services**, included traditional Telco ones
- **Network virtualisation** enabling network re-programmability & agile service creation

**Operation Model Change**

Global E2E vision instead traditional silo model, not linked to monolithic OSS

**Organization Model Change**

Breaking the traditional model mapping isolated network domains
DISCOVER_

DISRUPT_

DELIVER_

BE MORE_