"The goal is to focus on increasing profit per end-point when deploying IOT services."

NFV, KEY IOT ENABLER

INTRODUCTION

The proliferation of Internet of Things (IoT) end-points and the connectivity required for various verticals and solutions is exacerbating the profitability challenge for service providers and will continue to do so in the foreseeable future. The increase in operational complexity of service providers' networks is a major factor in exacerbating the average revenue per user (ARPU) and margin challenges. Service providers' infrastructures are not designed to handle the volume of transactions and scale of IoT deployments. New IoT traffic patterns and types, the need for ad-hoc[1] connectivity[2] and the need for carefully orchestrated and allocated storage, compute and networking resources have transformed the requirements for the service providers' infrastructures.

As service providers prepare their infrastructure to meet the IoT generated requirements, network function virtualization (NFV) can be a critical enabler and the logical option to pursue. NFV becomes a critical enabler because the resource efficiency and service agility provided by NFV is key to the service providers' ability to offering rich, integrated, managed IoT services and move beyond a pure connectivity play.

NFV is also a logical option to pursue for IoT because content service providers (CSP) are, for the most part, engaged in a software defined network (SDN)/NFV driven infrastructure transformation for some of their core service offerings. Using the same, common infrastructure to drive IoT related requirements is beneficial from an operational uniformity and simplification perspective as well.

Technology, Standards and Connectivity

The industry is debating (albeit mostly technical) standards definition and identifying the best suited technologies/platforms for various use cases and applications. And it is assumed that the industry will agree on some form of convergence and standards/practices/platforms. The resulting multi-vendor ecosystem and partner-centric approach will be a key factor in ensuring innovation in the pipeline.

LPWAN Standards & Platforms	NFV/MANO/ Infrastructure	IoT End-Points	Open Source IoT Projects (Small Subset)
• LoRA • Weightless-P (N, W, M) • SigFox • RPMA (Ingenu) • DRAT • 3GPP's EC-GSM, Cat-0,1, M1, NB-IoT • 802.15.4	• OP-NFV • ONOS • OpenDaylight • OpenStack • MANO • Open Source MANO (OSM) • OPEN-O • CORD-M (ONOS)	• SW-Defined Radio SDR • HW Reference Design and SDKs (Arduino, LinKit SDK v3, Arduino, Raspberry Pi) • Etc.	• Kaa (Cybervision) • Kura (Eclipse Foundation) • Predix (GE) • IoTivity (OCF) • Eddystone (Google) • OpenThread (Google)

[1] Possibly unplanned with high concurrency requirements.

[2] Centralized, decentralized, distributed, peer-to-peer.

Zigbee • BLE • 802.11ah • QoWisio • Etc.	• Service provider initiated (ECOMP AT&T/Orange) • Etc.		• Open Source Low Footprint OS • Etc.

Table 1. Noncomprehensive Examples of Competing Standards/Initiatives/Platforms Relevant to IoT in Various Forms

Economics

There is broad agreement that IoT exacerbates network operators' operational challenges (proliferation of end-points, peak versus average concurrency, high fan-out, hyper connectivity, etc.). The conversation about cumulative cost of operation alone, however, is a "cost per bit" conversation mostly centered on enabling the lowest possible connection cost and containing the exponential cost of operation for 100s of billions of end-points. This conversation is necessary but not sufficient. There must be an accompanying and complementary conversation about value creation, innovative new services, and new business models with improved agility.

A connectivity-only offering without strong emphasis on innovative and integrated managed service offerings will not be economically viable in the next three to five years, especially considering the operational costs of IoT.

Figure 1 demonstrates that the economics of "wait and see" are not a sustainable option for service providers. They need to create more profitable services.

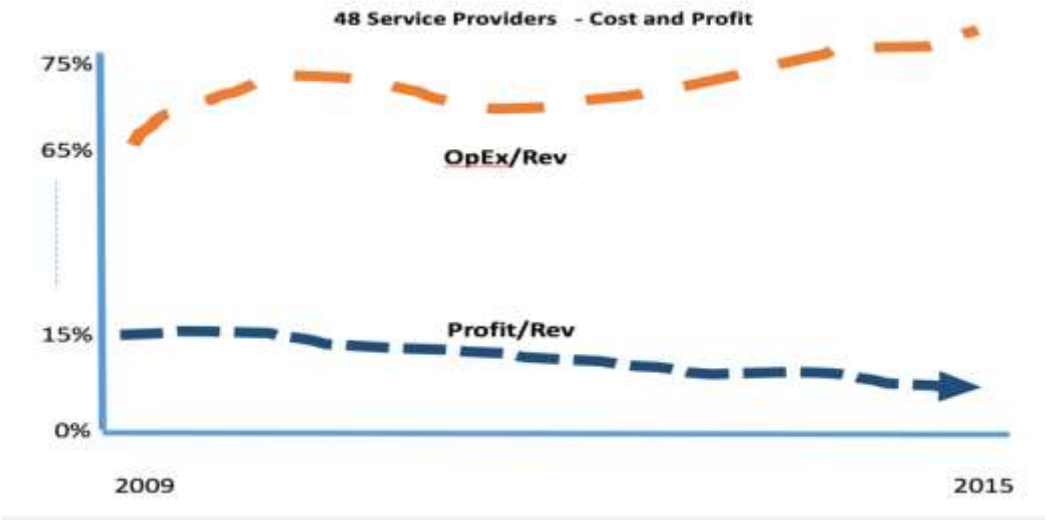

Figure 1. Economics of Wait and See

THE IOT SUCCESS INGREDIENTS

IoT is spurring new supply chains, value chains, and ecosystems across verticals, industries and even lifestyle brands (wearables, M-health, etc.) A variety of competencies and critical hardware, software and assets are required to successfully deliver a broad spectrum of managed applications and services either natively or through extensive partnering and ecosystem building. Table 2 is a list of IoT related services and the key requirements of those services.

	Desired Attributes: Competencies & Requirements	
IoT Solution Delivery/Industry Verticals/Customer Application	• Provides integrated, easy to manage, extensible • Delivers feature-rich apps • Delivers superior UX, UI	IoT End-to-End Security (Infrastructure, end-point, device, user, applications, data encryption, etc.)
Analytics, Dashboard & Visualization; Business Rules and Policy Definition	• Enables integration with rich, predictive analytics and AI tools • Enables RT and n-RT with programmable and intelligent events management, policy definition and enforcement • Enables rich dashboard composition and visualization tools • Reaches standards and protocol support (Zookeeper, REST)	
IOT APIs/API Repository & Catalog(s)	• Provide open and extensible catalogue • Enables fast service composition, assembly, delivery • Provides ease of integration and customization	
Data Management/Cloud DaaS	• Delivers massive scalability • Provides programmable, open, API-invoke-able • Enables RT (data streams) and n-RT stream support • Enables integration with sophisticated native + third party Machine Intelligence and Learning tools • Delivers rich platform support (Apache Spark, Cassandra, Kafka also Azure, AWS, Mesos, OpenStack, etc.)	
MANO/FCAPS/Controller/ Device Management	• Delivers standard, open, flexible, easy-t-integrate management • Delivers scalability	
IoT Platforms (IaaS and SaaS to an extent)	• Provides flexible PaaS/SaaS scalable • Enables ease of integration/SDK	
Core Infrastructure Storage, Compute, Networking, RF and Smart	• Delivers on premise (private), cloud-based and or hybrid • Provides hyper-enabler, elastic, scalable,	

Devices/Objects/Module	secure, feature-rich • Provides flexible and easy integration via open SDK • Enables CI/CD • Delivers predictive resource management (peak, average, critical event) • Supports devices for Open SDK and web-enabled, modular, extensible programmable environments, sensors & connectivity management	

Table 2. Competencies

NFV: KEY ENABLER FOR IOT DEPLOYMENTS

CSPs' infrastructures are not designed to handle the volume of transactions and scale of IOT deployments at inception. The NFV transformation, if realized properly, will allow SPs to build and optimize service delivery infrastructures around profitability and service requirements for IoT as opposed to building services to suit the hard network and infrastructure constraints (sometimes dictated by standards). The following are ways NFV will affect IoT deployments.

1. Flexibility of Network Functions and Architecture

    a. NFV and SDN based infrastructure implementation will allow service providers to look at compute, storage, networking, orchestration and all infrastructure assets (RF, end-points, POPs, etc.) as elastic, malleable and flexible assets that can cater to their comprehensive sets of services and revenue requirements. This will be the foundation that enables a service-oriented architecture in its true sense, where the network is designed and resources are allocated to meet service requirements.

    b. The ability to create multi-tenant networks (or isolated slices) for different applications is critical to the many business models that will be required to deliver IoT services.

2. Efficiency and Economics

    a. IoT platforms will deal with a scale of connections/devices that will run into billions with an average revenue per device that will be in cents. The ability to build platforms out of industry standard hardware and the ability to instantiate network functions when and to the capacity required will be critical in designing these platforms, mindful of the operational expenses and capital expenses in relation to the revenue intake. NFV and SDN have the potential to affect the economics.

    b. The capabilities highlighted in Table 2 need to be assembled and integrated to deliver meaningful managed IoT services. Creating compelling and profitable IoT services must involve the various capabilities highlighted across the supply chain. IoT is an ecosystem play. Equipment and platform manufacturers can be key catalysts to enabling and accelerating the movement toward higher value IOT services.

c. Service Composition Agility: The service agility components with NFV deployments (resource and service orchestration, updates to OSS/BSS, upgrades to assurance functions and self-healing capabilities, etc.) will contribute to the rapid service composition required for IoT services. The capabilities highlighted in Table 2 must be assembled and integrated to deliver meaningful managed IoT services. Creating compelling and profitable IoT services must involve the various capabilities highlighted across the supply chain. To create a profitable IoT service in an ecosystem players with different capabilities must come together to create services.

To illustrate the benefits of decoupling logical, virtual and physical assets, the following examples demonstrate how network operators can leverage the full potential of NFV and infrastructure "cloudification" to enable IoT services:

Example 1: Creating ad-hoc enterprise mobile virtual network operators (MVNO) with tailored resource allocation based on managed service with service level agreements (SLA)

Stringent security requires that a specific enterprise within a security and resiliency-conscious vertical and that the PDN-GW and S-GW VNF instances never reside on the same physical and/or logical resources as other subscribers or enterprises or require that specific, intrusion detection /firewalling and/or advanced security VNF instance is dedicated and load-balanced to cater to its corporate domain(s) only. At the opposite end of the spectrum, some price-sensitive and less SLA conscious customers may be open to resource pooling with a larger number of small businesses.

Specifically, this capability could translate into the instantiation of one lower SLA virtual network, for example, for city-wide smart lighting statistics collection (activated dynamically at nonpeak hours on idle servers); advanced (and dedicated, high-capacity) security capabilities could be used over the same smart lighting IoT network to ensure the critical elements of the energy infrastructure get the highest SLAs with dedicated and adaptive resource allocations across the attack surface to prevent cyber-attacks (leveraging advanced security analytics APIs on demand to prevent advanced persistent threats).

Without NFV, achieving the same goals would require the proliferation of specialized appliances, some requiring costly installation (truck rolls), interconnection (multiple times over), with possibly low resource utilization levels.

Example 2: Compute Capabilities at the Edge

Integrate compute capabilities within the eNodeBs to enable rich, advanced services and capabilities with faster response time thanks to local computing/decision making and therefore charge a premium price for the user's experience. Distributed content cashing and delivery for IPTV or over-the-top video, ultra-localized and targeted ad-insertion or the predictive instantiation of network functions, micro-services or of additional resources at the optimal location (centralized, decentralized or optimally distributed) for peak demand (performance or number of subscribers).

In effect, the MNO can look at the full range of compute-enabled eNodeBs (in the 10s, 100s of 1000s or millions, depending on countries) as very large distributed data centers at their disposal. Similar concepts of FOG computing or mobile edge computing run IoT enabling applications much closer (or farther away) to the end-points and in a much more scalable and/or optimized fashion.

This capability can provide IoT operators the ability to aggregate high rates of signaling data at the edge of the network and in many cases, aggregate traffic and process it at the edge and provide only the required information to the network functions or platform functions centrally located. When it comes to billions of devices, this is the only way to scale. This is an important requirement because many of the networks are not designed to handle the volume, scalability and the number of transactions required of IoT. Service providers need to leverage NFV in the infrastructure to make these services much more profitable. Some examples of those that have leveraged NFV have lowered their overall costs by 36%, capex by 29% and opex by 39%.

Example 3: Integrated Managed Services

Moving beyond connectivity often entails managing "IoT platforms." These IoT platforms include functions to manage analytics, mediation, repositories, stores, etc. They can also serve as an IaaS/PaaS base to onboard and offer third-party or end user driven applications.

With IoT platforms, service providers can enable various degrees of integrated managed services. Service providers can also adopt Internet as a service/platform as a service strategies that position them beyond connectivity with a focus on enabling IoT application repositories/stores/platforms/and environments that enable rapid IoT service composition (possibly API/cloud-based). Examples of invokeable modules or APIs that could be part of "a-la-carte" IOT services are communications service modules, power and energy and analytics.

NFV and enhanced orchestration solutions can enable rapid service composition capabilities that could, for instance, mash up four categories of APIs, to enable a joint venture between car manufacturer consortiums and regional or global service providers to not only enable, for example, self-driving electric cars with grid, and power station management (predictive supply management/failure avoidance), but also to enable video-conferencing and/or interactive ad-sponsored entertainment capabilities on-board that would be customized based on users' profiles. As the users get closer to a mall or a specific retail store, tailored offers, e-coupons and ads could be displayed based on location proximity and passenger profile(s).

CSP PERSPECTIVES

Verizon

David Vasquez, senior IoT specialist at Verizon, states the company has been monetizing its brand infrastructure for a long time. Verizon's idea is letting partners come to them and charge them for transport to use their highways, which has been very profitable for Verizon. But as things have progressed and technologies such as IoT are coming to light, Verizon has realized that it is not enough. For the company to be responsively profitable it realized that it should

move up the stack and that it is about the application and platforms. To address this, Verizon launched an IoT platform called Think Space to accelerate IoT development and go to market for the masses. Think Space is offered as a service from devices and is sensor agnostic and network agnostic. Verizon uses building blocks such as security and hosting on its cloud assets. The company is contemplating leveraging technologies such as NFV as a building block to help it intelligently manage.

Orange

Eric De Beau, head for R&D., Network Division, IT Solutions for the Core Network, Orange, indicated that with 5G it is clear with NFV, SDN, big data and analytics will be the key enablers. Orange is not waiting for 5G to be finished and has launched some IoT services, for example, sensors in France. The company not only launched the network but covered 18 Euroban areas and wants to target 120 by the end of January 2017. It also partnered with Venci to provide sensors to collect data to better service the maintenance areas. The company is also working with various sectors on IoT.

CONCLUSION

Service providers can lead and enable entire ecosystems if they adopt an "integrated managed services" approach to IoT. Service providers' asset strengths and know-how can be aligned with the requirements in key IoT industries, verticals, use cases, and "killer apps." The opportunity to offer platforms and services that are at the center of high-value service offerings is potentially theirs to lose as nimble content and application service providers develop various integrated IOT solutions "over the top" or potentially atop their own newly built infrastructures.

Service providers have a unique opportunity to fully seize the IoT opportunity and insert themselves within high-value IoT services supply chains. NFV can be a tablestakes technology to offer "right sized" cloud-like infrastructure, fast service assembly and delivery combined with measurable advances in elasticity, agility, service composition capabilities and cost structures that allow service providers to compete better with Amazon, Microsoft Azure, and Oracle IOT Cloud SDK offerings. Providers' existing connectivity assets are critical and possibly a great source of differentiation against content and application service providers and can be the underlying foundation of any high-value service deployment. Every IOT deployment requires a reliable, secure and scalable network that can run mission-critical applications. Service providers must look beyond connectivity and ensure that their plans integrate a panoply of high-margin IOT services.

The goal is to focus on increasing profit per end-point when deploying IOT services.