The Evolution of Public Cloud to Support Telco Network Functions
Executive summary

Over the last few years, the technology used by network operators to build network functions virtualization (NFV) infrastructure has evolved quite successfully to address the mission of NFV, namely to replace physical network appliances with virtual ones. But network operators have learned first-hand that building and operating this kind of NFV infrastructure is difficult and costly and that the right mission for the softwarization of their networks is not virtualization but cloudification. As both network operators and their vendors embrace cloud-native approaches to building and operationalizing carrier-grade network functions, the telco industry finds itself moving into alignment with the wider software world—a world that is embracing public hyperscale cloud as the natural home for most workloads.

Traditionally, network operators have responded to the needs of their network function use cases with purpose-built private cloud infrastructure. There is no question that network function workloads are unusually demanding. But public hyperscale cloud has been evolving quickly over the last few years and is now more than capable of hosting the great majority of network function workloads. Network operators now have a genuine choice between continuing to build, operate, and evolve their own infrastructures for network function workloads, and offloading responsibility for the infrastructure to public hyperscale cloud operators that bring enormous economies of scale to bear. Operators who take the latter course of action can focus all of their energies on the services that attract customers and generate revenues, rather than being consumed by building, maintaining, and operating infrastructure that is difficult, costly, and ultimately undifferentiated.
Introduction

In the eight years or so since the publication of the original white paper that coined the term “Network Functions Virtualization,” many lessons have been learned both by network operators and by the vendors that have historically provided them with network equipment. With hindsight, two key learnings stand out. First, the vision for NFV described in the white paper for the softwarization of network functions could have gone much further than a simple box-inspired model of virtualized software appliances and instead offered a comprehensive re-imagining of network functions for the cloud era. And second, the building and operating of cloud infrastructures suitable for hosting network functions and delivering carrier-grade services turned out to be far more difficult and costly than was expected.

In this paper, we explore the implications of those learnings and show how they lead inexorably to one conclusion: that in most cases, hosting network functions in public hyperscale clouds is the best way to realize the benefits of efficiency, acceleration of innovation, and targeted service offerings.
Current state of NFV
From the beginning of the NFV journey, most network operators sought to own and operate the cloud infrastructure that would host their virtualized network functions. In working with their vendors through the years, however, network operators discovered that the cost implications of operating in this manner exceeded their expectations. As vendors were required to make large investments to evolve their physical network appliances into virtualized software products, they passed these costs on to network operators. As a result, the NFV journey so far has not been as frictionless as either vendors or operators desired.

NFV infrastructure
There are two viable approaches to private NFV infrastructure: open-source solutions based on OpenStack or commercial cloud software solutions available from VMware.

Evolution of private cloud for NFV
Both OpenStack and VMware are essentially Infrastructure-as-a-Service (IaaS) solutions, designed to support server workloads in virtual machines supported by hypervisors. These solutions were designed to improve the economics of enterprise data centers. This was accomplished by the consolidation of a wide range of IT workloads that reduced the total number of host machines required to support them. Virtualized network functions vary widely in the demands they place on computing, memory, storage, and network bandwidth. Some of them, particularly those concerned purely with network control plane functionality, resemble IT workloads—and can therefore be migrated from dedicated appliances to virtual machines quite straightforwardly. Others, particularly those concerned with handling user traffic such as session border controllers, application gateways, routers, and firewalls, place much greater demands on network connectivity with respect to both bandwidth and packet throughput.

It is in this area that we see the greatest degree of private cloud evolution specifically to address NFV. Private cloud solutions have embraced technologies such as DPDK, SR-IOV, CPU pinning, and NUMA-aware scheduling to better support network-intensive VNFs.

The SDN layer
Every cloud stack needs to include a software-defined networking (SDN) component that provides secure connectivity between and among the workloads deployed by a given tenant while ensuring isolation of traffic between tenants.

In general, private clouds model their SDN function on a Layer 2 abstraction of the network. In effect, when you define a “network” in the private cloud to connect your workloads, you are defining a virtual Ethernet segment. This supports standard Ethernet semantics such as DHCP and ARP, and from the point of view of workloads, it behaves just as a physical Ethernet would.

A Layer 2 abstraction is well suited for use cases that involve virtualization of legacy software applications, many of which rely on some aspect of Layer 2 semantics for their proper operation. From its outset, NFV described a vision in which virtualized network appliances replace physical ones, so this looked like a good fit. And indeed, network functions that were
ported from their legacy physical appliance origins, where they relied on Layer 2 network semantics to support features such as fast failover, “just worked” when deployed in private clouds.

However, it is well known that physical Layer 2 networks do not scale well, and Layer 2 network abstractions in the cloud don’t scale well either. For this reason, none of the hyperscale clouds support a Layer 2 network abstraction.

Orchestration
It has long been recognized that achieving a high degree of operations automation is critical to the business case for virtualizing network functions. Operations automation requires orchestration, and orchestration turns out to be a very complex problem in practice.

The main challenges with orchestration pertain less to the cloud infrastructure and more to the workloads whose operations we want to automate. The problems arise mainly because the workloads were designed for a procedure-based operational model, which is inherently hard to automate.

Network functions
Most of the network functions that operators plan to virtualize (or perhaps have already virtualized) have been evolving for many years in response to new generations of standards and emerging operator requirements. As a result, they typically incorporate thousands of features implemented in many millions of lines of code. This code was originally written for a physical appliance environment, not a cloud.

Ported appliances
Given the complexity of typical network functions and the longevity of their codebases, it is not surprising that most vendors initially chose to approach virtualization by minimal adaptation of their software to run in a virtualized environment. But the ported appliance approach inherits many of the problems seen with physical appliances, including the need to double up on hardware to achieve fault tolerance, the difficulty of scaling a service to meet growing demand, and the challenges of operations automation with a procedural-based management model. These problems are a major obstacle to the goal of successful business outcomes from many network function virtualization projects.

Cloud-native applications
From the very earliest days of public hyperscale cloud services, software developers realized that the cloud enabled an entirely new approach to the design of large-scale fault-tolerant applications. These developers adopted a set of practices that have come to be known as “cloud-native,” embodying decomposition of complex applications to microservices, stateless scale-out architectures, declarative (as opposed to procedural) configuration models, and continuous integration/deployment build pipelines.

Web-scale players have very effectively demonstrated the value of a cloud-native approach by building highly resilient services that make efficient use of hardware resources. These services scale quickly and easily as demand grows while enabling rapid and non-disruptive service innovation and requiring minimal human resources for operational management. These are precisely the characteristics that network operators now realize they should seek from their NFV projects as ported appliances have been unable to deliver them.
It is certainly possible to build network functions according to cloud-native practices. The problem is that it requires a “clean sheet” approach to building the software. Re-factoring a complex software product that was originally architected as an appliance to one that properly embodies cloud-native practices is a huge undertaking and usually involves re-writing most of the code.

The benefits of a cloud-native approach to network function virtualization are now very apparent to both network operators and their vendors, and the industry is stepping up to deliver the next generation of virtualized network functions in cloud-native form, helped in part by the recognition of standards bodies, such as 3GPP, that cloud-native is the right direction. This will be transformative in terms of future return on investment in network virtualization projects.

Key challenges with NFV on private cloud
While the growing availability of cloud-native network function solutions will surely improve the prospects of future NFV initiatives by network operators, the infrastructure continues to present serious challenges.

Lifecycle management of cloud infrastructure
A private cloud stack requires a huge amount of software infrastructure that does little to improve the services delivered by the network function workloads that run on it. Yet, it demands a great deal of continuing investment of time and resources to keep it up to date. Private cloud deployments can be extremely difficult or impossible to upgrade without taking the entire cloud out of service. As a result, many NFV deployments are stranded on obsolete and no longer supported versions of cloud software, to which it is difficult or impossible to apply bug fixes and security patches. This is a big headache for network operators.

Performance of SDN
Most of the implementations of SDN in private clouds do a decent job of supporting IT and control plane workloads, which represent the majority of virtualized workloads that network operators have deployed to date in core data centers. However, they are challenged when asked to deal with workloads closer to the edge that process user plane traffic, such as Session Border Controllers, SAE Gateways, 5G User Plane Function, or Broadband Network Gateways. Many network operators obviate this problem by effectively bypassing the SDN layer completely and connecting workloads directly to the physical network fabric via SR-IOV. Still, this creates substantial management challenges and makes it difficult to comply with Zero Trust security directives.

Continuing growth in complexity
The virtualization of ported appliances relies on hypervisor-based environments supporting virtual machines. But cloud-native network functions expect a container-based environment orchestrated by Kubernetes. The transition to cloud-native will take a number of years, during which both models will need to be supported. Having to support a Kubernetes environment on top of, or alongside, a Virtual Machine environment will add yet further to the operational challenges of private cloud for NFV.

“A private cloud stack requires a huge amount of software infrastructure that does little to improve the services delivered by the network function workloads that run on it.”
Hyperscale clouds

Although the original intent of the OpenStack community was to build a cloud stack that offered equivalent function to public hyperscale clouds, the fact is that private and hyperscale clouds differ today in some quite fundamental respects. A key question for the industry is whether these differences make public hyperscale clouds more or less suitable for hosting telco network function workloads.

One of the most obvious differences between private and hyperscale public clouds is the level of investment that has been made in the overall cloud stack. The sheer scale of the leading public cloud businesses drives massive investments in the technology and the talent to build clouds. As a result, public clouds today are more feature-rich, reliable, efficient, performant, scalable, and secure. Furthermore, they can be managed, maintained, and operated at a significantly lower cost.
Characteristics of hyperscale cloud

**Compute**
The private NFV cloud is fundamentally an IaaS solution, focused as it has been on the mission of supporting network function appliances. But the new generation of network functions will be cloud-native, requiring support for containers and Kubernetes. Hyperscale clouds such as Azure have mature and well-integrated support for Kubernetes clusters, together with additional supporting technologies such as service mesh. Hyperscale clouds also support an even newer compute paradigm – serverless – which offers some very interesting future possibilities for rapid innovation in telco network function workloads. In evolving beyond its original IaaS mission to support the next generation of cloud-native workloads, private cloud has a great deal of keeping up to do.

**SDN**
Software-defined networking is certainly one of the more complex aspects of the cloud. While OpenStack supports a multiplicity of plug-in SDN solutions, none of them are ideal for supporting the full range of telco network function workloads. On the other hand, the hyperscalers have invested very heavily in both software and hardware offload technologies in order to create highly performant industrial-grade SDN solutions. For example, Azure Accelerated Networking makes use of a Microsoft-developed SmartNIC equipped with FPGA for fast path offload that offers workloads wire-speed network performance while applying rich policy capabilities in support of Zero Trust networking.

One important difference in SDN between hyperscale and private clouds is that hyperscale clouds support IP-based connectivity but without Layer 2 semantics. This allows for massive scalability of virtual private networks within hyperscale clouds, but it does have certain implications for virtual private network appliances. We will discuss this topic below.

**Platform services**
Perhaps the most obvious and visible difference between hyperscale clouds and private clouds is the breadth and depth of platform services that are offered by hyperscale clouds. A quick glance at the Azure Directory of Services demonstrates this very well. There are many ways in which network operators can leverage these platform services very effectively in support of network function workloads, but we will highlight two examples here to illustrate some of the possibilities.

Some network functions require large-scale storage. Voicemail is a good example. Deployed in private cloud, a voicemail solution would need to incorporate its own storage function for voice messages. The network operator would have to maintain the associated storage software and manage the storage function itself to provide geo-redundancy, backup, scaling, and so on. In hyperscale cloud, a voicemail function can store messages in a database provided as a platform service, for example, Azure Cosmos DB. This is a well-proven, globally scalable, distributed, and geo-redundant database that is managed by Azure. Offloading the storage function to a managed database service such as Cosmos DB makes the overall voicemail software solution far simpler and greatly reduces the operational burden on the network operator.
Many network functions can benefit from Machine Learning (ML)/Artificial Intelligence (AI) to ingest analytics and generate actionable insights. To leverage ML/Al in the context of private cloud requires big investments in software with very uncertain returns. It is quick and easy for network operators to experiment with ML/Al in hyperscale cloud because of the wide range of such capabilities that are available on-demand as part of the platform. In developing their usage of ML/Al to improve operational efficiency and customer retention, operators can embrace a “fail fast” approach to innovation, enabling them to try new ideas rapidly and with very low capital risk.

**Security**

It’s not unusual to hear security concerns raised as one objection to hosting telco network functions in public cloud, but security vulnerabilities of the private cloud may well be of greater concern to network operators. Microsoft alone invests over $1 billion annually in cybersecurity and employs over 3,500 full-time security experts. This dwarfs the level of investment in security that could be afforded by even the largest network operators. Deploying network functions in hyperscale cloud will actually make it easier for network operators to comply with increasingly stringent government requirements for security than going it alone on private cloud.
Support for Virtual Network Appliances

Hyperscale clouds offer a wide range of Virtual Machine SKUs that are suitable for the deployment of virtual network appliances. Experience has shown that most such appliances can be run on hyperscale cloud VM services with little difficulty. However, the different SDN environment in hyperscale clouds may have impacts on network appliance workloads in two specific areas: failover and VLAN trunking.

HA and Failover

Many virtual network appliances inherit the fault tolerance mechanisms embodied in their physical forebears, and these often rely on Layer 2 semantics in the network to which they are connected. To achieve high availability, network appliances are typically deployed as active-standby pairs, with a virtual IP address that may be moved from active to a standby instance in the event of a failover. The migration of the virtual IP address may be accomplished by having the newly active member of the pair issue a gratuitous ARP to associate the virtual IP address with its MAC address in the ARP caches of its neighbors. Alternatively, network appliances can leverage routing protocols such as BGP to accomplish the migration of virtual IP addresses between active and standby instances.

The load balancer itself can detect the failure of the active instance and initiate failover; alternatively, the network function workload can be made responsible for detecting the failure and calling an API on the load balancer to force the switchover. Either way, a small amount of enhancement work to the network function software is likely to be needed.

VLAN Trunking

A small number of network function types, including Broadband Network Gateways and Session Border Controllers, may need network connectivity that supports VLAN trunking. What this means is that they natively process Ethernet packets that include 802.1Q VLAN tags, which are typically used to distinguish between different customers in the access network.

Hyperscale clouds don’t support VLAN trunking. But there is a simple workaround: 802.1Q VLAN-tagged Ethernet traffic can be encapsulated in the telco network before being sent to the network function in the hyperscale cloud. VXLAN encapsulation is the recommended way of doing this. Most of the routers deployed in telco access networks can be configured to encapsulate Ethernet traffic in VXLAN, so no incremental investment is normally needed. However, the virtual network function software will need to be enhanced to support VXLAN-encapsulated traffic.
Support for cloud-native applications

With cloud-native network functions, the rich platform capabilities of hyperscale clouds really come into their own. Properly architectured cloud-native network functions take care of fault tolerance and scaling with stateless microservices, backed by scalable, fault-tolerant state stores—which may themselves be based on managed database services such as Azure Cosmos DB. The Kubernetes clusters into which cloud-native network functions are deployed may take advantage of managed services, such as Azure Kubernetes Service (AKS), which comes with its own CI/CD pipeline for rapid innovation with managed canary testing of new software builds. The development of new cloud-native network functions becomes even simpler with managed service mesh functionality such as Azure Service Fabric, which offloads responsibility for load-balancing and critical security functionalities, including mutual authentication and encryption on microservices interfaces.

While the platform capabilities of hyperscale clouds make it far easier and quicker to develop carrier-class cloud-native network function applications, vendors of such applications may push back on the basis that each hyperscale cloud is different, and they cannot afford to build versions of their apps to suit each different cloud.

One of the most important principles of cloud-native architecture is a technology-neutral approach to microservice implementation. A microservice should be implemented so as to expose APIs that are independent of the underlying technology on which the microservice is built. This allows the maintainers of a microservice to substitute different technologies in the future without affecting the consumers of the microservice by retaining the same APIs.

If properly adhered to, this principle makes it easy for developers of cloud-native network functions to support portability across different hyperscale clouds. For example, a microservice designed to store state on behalf of stateless microservices in a 5G control plane would be constructed with a technology-independent state storage API layer on top of a hyperscale platform cloud database service such as Azure Cosmos DB. This API layer should be lightweight and quick to develop. To port the solution to a different hyperscale cloud, the API layer would simply need to adapt to suit the equivalent database service in that cloud. The semantics of the various cloud database services, be they SQL or NoSQL, are broadly similar across hyperscale cloud providers, and the differences can easily be abstracted away with the appropriate access API layer, so achieving portability between clouds should not be difficult.

"A microservice should be implemented so as to expose APIs that are independent of the underlying technology on which the microservice is built."
Hyperscale at the Edge

In general, it is fair to characterize hyperscale clouds currently as highly centralized and served out of a relatively small number of geographic locations in any given territory. For network operators who are looking to deploy virtualized network functions associated with their service’s edge, such as 5G UPF, BNG, or content caches, it’s not immediately obvious that hyperscale cloud has anything to offer to meet this need.

Recognizing the specific needs of workloads such as 5G UPF, the hyperscale cloud providers are making a variety of solutions available that bring the benefits of hyperscale to the operator network edge. These range from lightweight solutions that simply extend the reach of hyperscale management portals into private edge clouds (e.g., Azure Arc enabled Kubernetes) to full-stack edge clouds that include all the hardware and software needed to replicate the hyperscale environment at an appropriate scale for the edge (e.g., Azure Edge Zones).

Hybrid cloud is a well-established approach for enterprise apps, allowing software systems to be deployed across a mix of public and private cloud facilities. Solutions like Azure Arc are intended to make it as easy as possible to manage such applications in a consistent manner from a single pane of glass. Perhaps the best way for network operators to view their edge cloud facilities is as an expression of hybrid cloud, where software systems such as the 5G packet core are distributed between edge cloud locations and centralized public cloud. The 5G architecture, with its support for Control and User Plane Separation, lends itself well to this kind of approach. The UPF is deployed in private edge cloud instances, while the control plane, including AMF, SMF, AUSF, and UDM, can reside in the public cloud. Azure Arc can provide management visibility and control across the entire system.

The edge also offers outstanding opportunities for partnering between network operators and hyperscale cloud providers. With network operators bringing their central office real estate and local mobile and fixed broadband access network connectivity, and hyperscale cloud operators bringing their IoT platforms, edge computing applications, and developer ecosystem, all of the moving parts necessary to exploit the capabilities of 5G in the new era of edge applications come together under a telco/hyperscaler partnership. Then the question arises: is it necessary to have two distinct cloud stacks at the edge: one to support telco network functions, the other to support third-party edge applications? We have found that a single edge cloud stack, based on hyperscale technology, is quite capable of doing both. Therefore, looking at the longer term, we believe the best approach is for network operators to embrace hyperscale at the edge, as well as in the core.
Challenges with public cloud

In this paper, we argue that the technical obstacles to a successful deployment of network functions on public hyperscale clouds, which have traditionally been the central objection of network operators, have become minimal and are now easily surmounted.

Other objections would have been on business grounds. For example, many network operators began the NFV journey expecting it to cost less to host their network functions on private cloud than on public cloud. But as data about the real costs of owning, operating, and maintaining complex private cloud infrastructures emerge from hard-earned experience, more and more network operators have realized that infrastructure cost actually favors public cloud.

The third main category of objections would have been around regulatory concerns. Prime amongst these would have been data sovereignty. Governments have legitimate concerns about the private data associated with users of regulated telecoms services being stored on systems located outside of their national borders, not to mention highly sensitive information such as Lawful Intercept warrants. With public cloud revenues growing at rates of around 50% per annum, hyperscale cloud operators are investing heavily to build out new data centers and establish a local presence in more and more territories. Where network operators do not have the luxury of a choice of local hyperscale cloud providers, they can usually address the problem of data sovereignty with suitable hybrid cloud solutions that maintain sensitive data storage within their own private clouds.

Governments are also increasingly sensitive to security concerns around telco networks. In recent interactions with government departments on this topic, it has become clear that government security experts have fewer concerns about the security of hyperscale clouds than that of private clouds owned by network operators. This reduction in concerns is mainly because of the scale of resources available to hyperscale cloud operators and their demonstrated world-class expertise in cybersecurity.

Many network operators work in a highly regulated environment, where, for example, a voice services outage may need to be reported to a regulatory authority and may actually result in a punitive fine. This is certainly an important consideration for network operators who are exploring the hosting of such services in hyperscale clouds, where a service outage may result from an infrastructure-level failure that is outside their control. Of course, any cloud-based service is at risk of disruption from failures in the infrastructure, whether the cloud is public or private, and it is incumbent on both network operators and the vendors of their network functions to architect complete systems that are maximally tolerant of faults in the underlying infrastructure. At the same time, hyperscalers clearly need to demonstrate a track record of excellence in platform availability.
Evolution to NFV on hyperscale clouds

No matter how convincing the arguments for hosting network functions on public hyperscale clouds, the fact is that most network operators have already made sizable investments in private cloud NFV infrastructure and have already onboarded a substantial number of network functions. How, then, can network operators effectively transition towards hosting network functions in hyperscale public cloud?

The best starting points for the journey to network function hosting in hyperscale cloud can be found at the two opposite ends of the network function adoption lifecycle.

At the trailing edge, we have network functions that have been in the network for many years and are yet to be virtualized. These are often physical network functions that are near or at the end of life and need to be replaced—ideally, by cloud-native applications. At the leading edge, we have brand new network functions, often representing some new generation of technology. These network functions embody a cloud-native architecture, and as such, are easy to onboard to hyperscale cloud.
Trailing-edge applications

Voicemail is an excellent example of a trailing-edge application. In most networks, voicemail is still handled by aging physical appliances. Voicemail is not a revenue generator in its own right, nor is it a source of service differentiation. Subscribers' awareness of voicemail is mostly just an expectation that it will be there. Not surprisingly, network operators find it hard to get enthusiastic about virtualizing voicemail. Nevertheless, something should be done to replace these legacy systems.

Public hyperscale clouds are good homes for such trailing-edge applications. Although important to subscribers, they are not seen as super-critical and are therefore good candidates for “testing the water” in public cloud hosting. And in the case of voicemail, substantial operational savings can be achieved by offloading the storage function to an appropriate platform service such as Azure Cosmos DB, making storage management, backup, and disaster recovery easier.

Leading-edge applications

In the 5G network function space, we see two parallel and somewhat independent streams of activity: 5G as an evolution of LTE, offering greater coverage density for mass-market mobile broadband at lower cost and with higher speeds; and 5G as an enabler of multiple new classes of applications, mostly in the M2M space.

Most operators are addressing the enhanced mobile broadband use case for 5G initially with enhancements to their existing LTE network functions, many of which are likely already virtualized in private cloud. There is no obvious reason to consider transitioning these network functions to public cloud at the moment.

However, both operators and vendors have realized that the new M2M and edge computing applications enabled by 5G demand a different approach to the network functions needed to support them. Vendors are delivering genuinely cloud-native implementations of the 5G standalone packet core to suit the needs of these applications. Operators are looking for deployment approaches that enable them to move quickly and opportunistically to address emerging new use cases without having to plan for multi-year investments to build the necessary infrastructure. Public hyperscale cloud is a great fit for new deployments of 5G network functions intended to support edge computing and M2M applications because it enables network operators to stand up complete 5G packet core solutions quickly and with almost no up-front investment. We have already noted that hyperscalers are growing their presence at the edge, and this enables network operators to leverage public cloud to deploy distributed 5G core solutions with centralized control planes and localized user plane functions.

By leveraging public hyperscale clouds such as Azure, network operators can engage far more effectively with fast-moving 5G M2M and edge computing opportunities at far lower risk.
Looking forward

Summary and conclusion

In the beginning, NFV was about replacing telco network hardware with software. But once you start building networks in software, you come to understand that network functions are just another kind of software application, and therefore subject to the same evolutionary pressures as any other kind of software application. Over the last few years, those pressures have resulted in the movement away from software appliances to cloud-native architectures, the movement away from virtual machines towards containers, and the growth of public hyperscale cloud as the optimum environment for hosting a great many workloads. Private cloud is not going away any time soon, but public cloud is growing much faster—and with good reason. Most network operators are already running many of their IT workloads in public cloud. We suggest that it is now time for them to consider the significant benefits of running their network functions there as well.