market brief

NFV information as a service making virtualization practical, simple and telco-grade

Network Function Virtualization (NFV) promises unprecedented technological flexibility, business agility and savings. But so far, service providers are frustrated by its complexity and cost. There are thousands of potential Network Function Virtual Infrastructure (NFVI) and Virtual Network Function (VNF) combinations from dozens of vendors. This complexity increases the cost and lead time for developing and deploying network services, as well as the risk that errors will make those services unreliable.

No wonder some analysts describe NFV as "the Wild West."[1] Standards bodies are working to address the onboarding challenges caused by the disparate industry standards, which lack coordination. Standards development and open-source options also need to be harmonized.

4 roadblocks to virtual networks

There are four major reasons why service providers aren't transitioning to virtual networks as quickly and as smoothly as they hoped:

1. multi-vendor integration is tricky.

Network functions traditionally follow a tightly coupled vertical architecture, where the service provider chooses a single vendor. Virtualization transforms this into a horizontal, multi-vendor environment. For example, a cloud stack could include four different vendors' hardware, VNF software, Virtual Infrastructure Management (VIM) layer and orchestration layer. The freedom to pick best-of-breed solutions from multiple vendors comes with the challenge of making them work together seamlessly and reliably.

2. vendor maturity is low.

NFV is a relatively new paradigm, so its vendor ecosystem is still developing. As a result, service providers have to do far more rigorous testing to ensure that each vendor's solution performs as advertised. That's in addition to testing to ensure each solution integrates seamlessly with the rest of the stack.

3. security is more complex than ever.

In a traditional architecture, service providers already struggle to stay ahead of emerging attack vectors and vulnerabilities. Virtualization is a new concept with a steep learning curve and more, often young vendors. The use of open source also eliminates telecom's traditional strength of "security by obscurity." Finally, the vendor ecosystem has been slow to provide the out-of-the box VNF security solutions that service providers need.

4. new skills are required but scarce.

VNF security, integration, testing and other virtualization-related tasks require new skills, which are in short supply industrywide. Existing team members across all functions—network, operations, support and even procurement—also need to acquire the new skills necessary as their environments transition from hardware to software.

[1] https://www.lightreading.com/gsma-to-bring-standardization-to-nfvi-wild-west/a/d-id/752467?

Some types of communication service providers have additional challenges. For example, network slicing is a fundamental part of fifth-generation (5G) mobile technology. A communications service provider eventually could have hundreds of slices, each one serving a specific use case, such as autonomous vehicle navigation or first responder drone video. Each additional slice and each additional use case increases network complexity for mobile service providers.

A mobile service provider could have multiple VNF providers for each slice. Manually ingesting software from that many vendors is complex and time consuming, and in turn delays each slice's time to launch and time to revenue. Automating and standardizing that onboarding process is the best way to minimize both the lead time and expense, and, in turn, provide the agility that service providers require.

Onboarding automation is particularly important for highly price-sensitive markets like IoT and highlights why zero-touch automation is a goal for service providers. The harmonization of standards activities with open source initiatives is an important step toward achieving this goal. Service providers need a neutral third-party verification that the cloud stack components (VNF, NFVI, orchestration layers) all function as designed and follow industry standards. The onboarding automation solution should have three components:

1. Leverage open source assets including ONAP and OPNFV.
2. Support existing ETSI, GSMA and MEF Forum standards wherever applicable.
3. Support operator-specific verification criteria.

activating VNFs in a service provider environment

onboarding

VNF image and artifacts will be onboarded to the cloud. Includes the verification of the VNF artifacts to validate if the VNF could be instantiated on the cloud.

instantiation

NFV MANO / ONAP orchestrator can use the VNF on the operator cloud. The VNF can accept some health checks as part of this.

configuration

Configuration of the VNF to allow the VNF to accept traffic on the network. May involve the Specific VNF Manager working with a NFVO.

testing

Testing the VNF for functional and performance aspects. This includes using traffic generators for functional and performance testing.

the cycle is repeated for VNF patch and new software releases

leverage automation for service agility

Although service providers want zero-touch automated VNF onboarding, this ideal remains elusive for a variety of reasons, including the aforementioned four roadblocks to virtual networks. Partners can help apply service provider-specific standards to validate and test VNFs and allow them to operate and innovate at scale. Verifying whether each vendor's implementation complies with standardized interface would reduce vendor lock-ins and enable standardized interfaces within the cloud stack.

Ultimately, the ideal onboarding automation platform provides four major benefits. Whether you use customer care trouble tickets, fraud alert systems or review traffic reports and profitability margins, complementing your existing fraud strategy with proven tools should allow for:

simplicity:

Today, service providers often turn to consultants and other third parties for help with implementing virtualization. With an automation platform, service providers can quickly and easily verify, install and integrate VNF and NFVI combinations on their own.

structure and consistency:

An automation platform provides a unified business process for deploying virtual systems. This includes ensuring that each system conforms to standards and best practices, and undergoes the appropriate tests for reliability, performance and a great user experience.

faster release cycles:

Simplification, structure and consistency enable faster release cycles. Now, service providers can develop and deploy network services at the speed of business rather than the speed of technology — or when a consultant is available to help. And the faster a service comes to market, the sooner it's driving revenue and providing market differentiation.

savings:

The more VNFs that a service provider has, the higher its overhead costs. When virtualization is simplified and standardized, the overhead cost of developing and delivering those services decreases significantly.

introducing iconectiv TruOps NFV information as a service

The iconectiv NFV platform enables all of these benefits. This cloud-based information service is integrated with the Linux Foundation's Open Network Automation Platform (ONAP), first included in the ONAP Dublin release. The solution is very modular and can easily be extended to integrate with non-ONAP orchestrators using APIs. It combines industry- and service-provider-specific test cases to streamline the compliance, validation and performance aspects of VNF onboarding.

This Information as a Service (IaaS) plug-in can combine industry-specific and service provider-specific verification criteria to help streamline and speed up the compliance, validation and performance testing for VNF onboarding. iconectiv TruOps Virtual is a VNF information service that is a simple, seamless and secure way for service providers to launch new network services. It helps different virtual network functions from multiple vendors speak the same language with speed and simplicity, which saves service provider costs, accelerates revenue generation, improves customer satisfaction and deliver a faster return on investment.

about iconectiv

Your business and your customers need to access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services and its unmatched numbering intelligence helps you do just that. In fact, more than 2B people count on our platforms each day to keep their networks, devices and applications connected. Our public and private clouds provide Software as a Service (SaaS) and Information as a Service (IaaS) solutions that span network and operations management, numbering, trusted communications and fraud prevention. For more information, visit www.iconectiv.com.

make the connection.

For more information about iconectiv,
contact your local account executive,
or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com