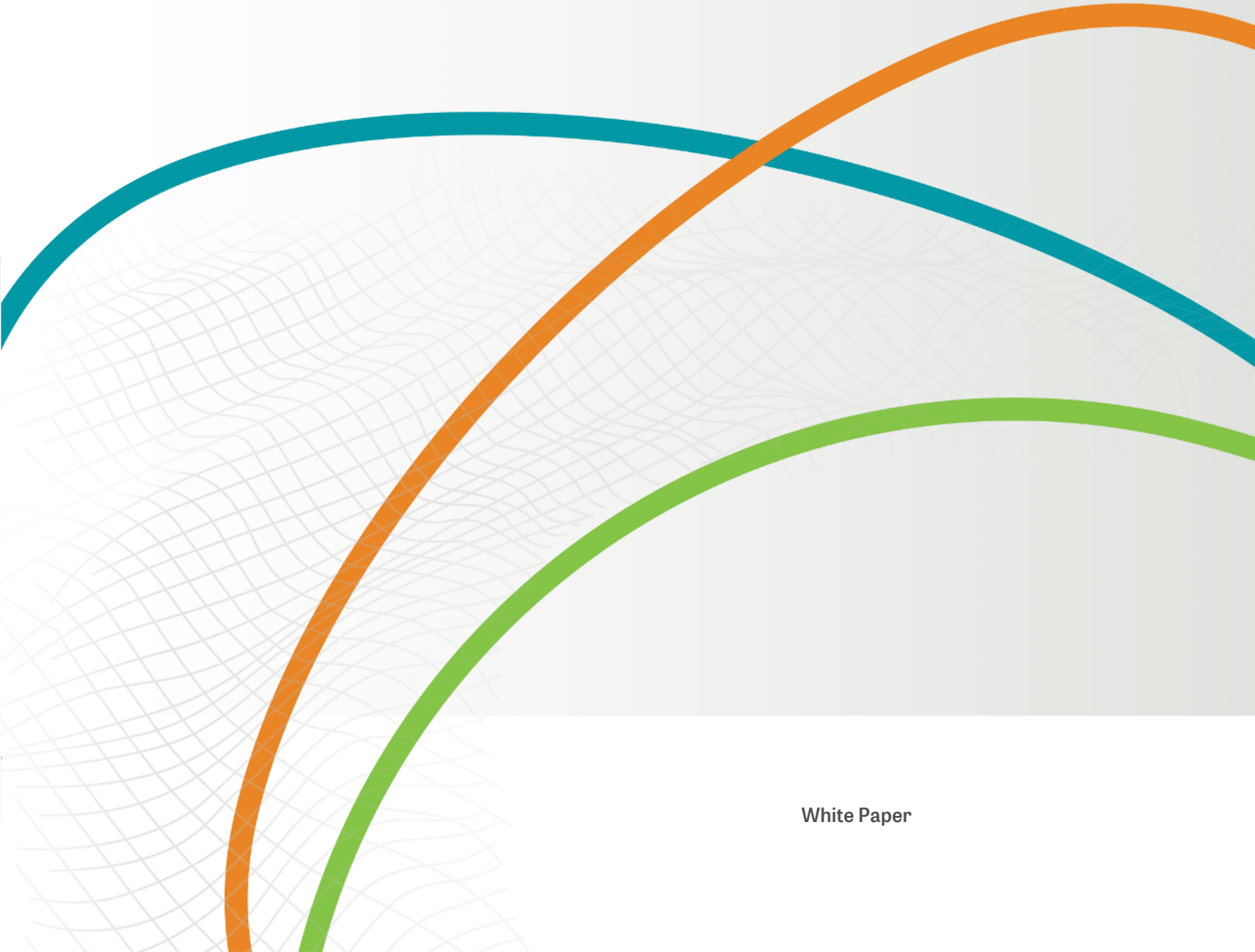
NFV: Beyond Virtualization

Virtualization by itself is not enough to deliver the full potential and value of the NFV architecture. Service provider costs and complexity increase with virtualization alone. Realizing the benefits of NFV requires a management and orchestration system to enable an adaptive network infrastructure.



White Paper

Realizing the Benefits of Network Virtualization

The service provider community is showing significant and growing interest in network functions virtualization (NFV) solutions. Service providers are looking to build on the groundwork put into place by cloud and software defined network (SDN) initiatives to augment the virtualization technologies of core service provider network services and functions. As service providers continue to define and drive towards NFV architectures, their interest has generated a lot of discussion surrounding the value of different aspects of NFV and what is required to realize the benefits NFV is designed to deliver.

As noted in the original NFV white paper from the European Telecommunications Standards Institute (ETSI)1, the virtualization of functions can potentially reduce capital and operational costs, increase service agility, reduce time to market, deliver a common and consistent infrastructure for multiple applications, and introduce innovation by creating an open ecosystem that encourages new industry participants. As service providers and vendors look at the details of implementing NFV and accomplishing its stated goals, however, they're raising concerns about the realization of some of these goals and whether implementation translates to the benefits initially expected.

Virtualization adds an extra layer of software and management through the virtual hosting infrastructure. While providing agility for improved service availability and reliability, it significantly increases the complexity of managing the infrastructure. Thus corollary technologies are needed to start benefiting from the virtualization of the core network services:

- Application Delivery Controllers (ADCs) provide the load balancing necessary to take advantage of the dynamic growth and flexibility of a virtualized network function (VNF).
- Intelligent DNS services through global server load balancing (GSLB) deliver the abstraction of the virtual network function (VNF) applications made available through the virtualization of provider services.

Operationalization is also critical to the success of NFV. A management and orchestration infrastructure that can control the NFV infrastructure (NFVI) and disparate virtual network functions is essential to deliver the full benefits of the virtualization technology. This management and orchestration system should be able to coordinate, with an autonomous intelligence, the VNFs via the VNFI to deliver the reliability, availability, and scalability expected of the NFV architecture.

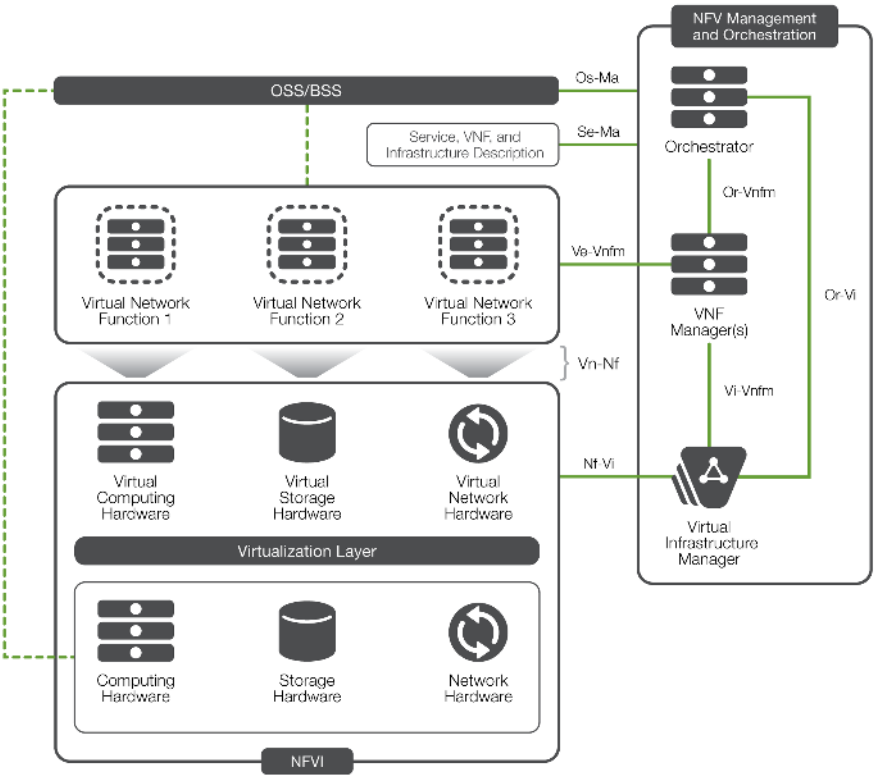


Figure 1: An intelligent management and orchestration infrastructure is critical to effectively capturing the benefits of NFV[2].

Demystifying NFV Benefits

As a result of moving network functions and services to software using commercial, off-the-shelf (COTS) hardware combined with standard or open APIs, NFV is expected to provide the following key benefits:

- OpEx and CapEx savings
- Service/network function deployment flexibility
- On-demand, elastic capacity and performance scalability
- Service velocity

In August 2013, F5 published a white paper[3] that outlined four components that are essential requirements for actually deriving the value of the proposed NFV framework: virtualization, abstraction, programmability, and orchestration. These four functions enable service providers to achieve the vision behind NFV, and the NFV framework to implement them is helping to establish NFV as an essential service provider architecture.

A consistent and unified architecture enables CapEx savings by allowing use of a single COTS hardware platform. There is a distinct cost benefit to a common COTS model for deployed applications and services. Unfortunately, when the model is analyzed from a cost/performance perspective, the benefit of virtualization is not as clear. Vendors optimize their software and hardware to work most efficiently together, so when they are not together, there is usually a significant performance loss relative to the cost of the combined components. Depending on the service and performance requirements, it may cost two to 10 times more upfront to deploy certain VNFs because of the additional licenses and COTS hardware necessary to meet network requirements.

From an OpEx perspective, the initial NFV vision does not look as promising as expected, either. Virtualization of services and the deployment of VNFs actually increase operational complexity by adding a virtualization layer to every VNF. It is then necessary for operational staff to understand and manage the virtualization infrastructure in addition to the services and applications. Operationally, since the services and applications are virtual and will be dynamically deployed to meet network demand, it is likely that the VNF forwarding graph will change as network resources are allocated and deployed. This places a large burden on operational staff to understand the service provider network architecture in real time. They will need to be able to manage and support a dynamically changing, complex network environment.

Of course, the lack of monetary benefits from the introduction of NFV into the service provider infrastructure does not mean that there is not a clear beneficial vision and reason to implement an NFV framework. It is essential for service providers to look beyond the basic virtualization of the services and applications, however, to see the full potential and value of NFV.

F5 Vision for NFV

F5 experts see NFV as a movement to capture the benefits of cloud and SDN architectures within the service provider network environment. Existing ADC technologies such as load balancing and global server load balancing are essential for NFV to succeed. In addition, service providers need to establish an orchestrated environment to extract the benefits of a virtualized service infrastructure.

A virtualized infrastructure offers service providers the framework for a more scalable, reliable, and flexible architecture, but the virtualization of services and applications through the use of VNFs does not by itself deliver these benefits. ADCs are necessary to deliver load balancing technologies for local scalability and reliability. The performance limitations of COTS hardware versus vendor-optimized hardware platforms also typically require service providers to combine the physical resources within a virtual pool through load balancing technologies, which also can provide automated fault detection, high availability designs through active/standby models, and the flexibility to add and remove resources within the virtual pool without service disruption.

Removing physical or geographical context from the delivery of core services is critical to extracting the benefits of an NFV architecture, and service providers can abstract their core services through advanced ADC services. In addition, advanced, intelligent DNS services extend beyond a physical location to deliver GSLB technologies to provide availability and fault tolerance at the global level. VNF graphs can be intelligently manipulated based on resource availability and the best path for delivering a service. The failure of a physical location or data center can initiate the redirection of sessions to an alternative location where services are available.

There is a strong need to scale an NFVI, since most individual VNFs cannot meet the performance needs of service providers. It is not economical to deploy a VNF per subscriber and per function, since the resulting VNF footprint is still too large. Yet if it is possible to consolidate various functions into a single VNF or converge multiple subscribers or offerings into a single VNF element, this element needs to scale. ADC technologies can increase performance linearly with the number of VNFs performing an identical function to limit the overall administrative overhead. This will also help to deploy cost-effective and performance-based solutions for aggregated traffic scenarios like S/Gi firewalls, where there is a strong need to disaggregate traffic.

Orchestration is the ticket

Without orchestration, the management and deployment of VNFs becomes an onerous and manual process. Orchestration delivers the framework to automate the benefits of a virtualized environment. This automation is essential for the creation, management, and adjustment of VNF forwarding graphs and for the creation and allocation of VNF resources.

F5 is proposing an orchestration architecture and framework as an overlay to NFV. An adaptive network infrastructure (ANI) orchestrates multiple VNFs and network elements through the collection of key real-time metrics, analysis of those metrics from multiple and disparate elements through advanced heuristic models, and adjustment of the network infrastructure to adapt to changing conditions based on operator-defined policies. Standard and open APIs are necessary to incorporate multiple elements into a centralized orchestration infrastructure. An orchestration engine, such as F5® BIG-IQ®, needs to collect data from different VNF components and understand the correlation of the different data points. Operator policies are applied to this data to determine whether the NFVI is within normal operational parameters. If an aspect is outside the scope of the operator policy, the orchestration engine needs to automatically enact policy changes to the network infrastructure to bring the service provider environment back within nominal operating parameters.

This dynamic infrastructure is akin to a biological ecosystem, with disparate elements that interact with each other in various ways. Events create external influences of various combinations upon these elements, and a reaction or adaptation is generated to normalize or mitigate the event.

Dynamic service chaining is a good example of how ANI can automatically adapt to changes in the network environment. Service chaining by itself is not a new concept, but in the past, building a service chain or NFV forwarding graph to support a new application or to build differential services took significant time and effort. It meant acquiring network devices and cabling them together in the required sequence. Each service required a specialized hardware device that had to be individually configured with its own command syntax. The risk of error was high, and a problem in one component could disrupt the entire network. Overall traffic flow was usually suboptimal because the effort required to construct a chain also meant that chains were often built to support multiple applications. As a result, data sometimes passed through unnecessary network devices or servers while consuming extra bandwidth and performance. Devices needed to be sized to support maximum demand—which might only occur rarely—and that meant excess capacity and therefore an underutilized capital investment most of the time.

With NFV-based technologies, the operator is able to productize the chain faster and more simply. Moving network functions into software means that, with proper orchestration, building a service chain no longer requires acquiring hardware. Network functions typically execute as virtual machines under control of a hypervisor. When more bandwidth is required, an additional virtual machine can be automatically provisioned to take part of the load. There's no need to overprovision VNFs, since additional server-based capacity can be added when needed.

ANI allows the NFVI to set up the service chain, which can consist of different hypervisors; different provisioning stacks, such as OpenStack and VMware; or both. This enables the operator to build a wide variety of NFV forwarding graphs focused on different data types and applications that are tuned for each scenario. The operator can also build location-independent chains, including technologies like routing based on geolocation.

Finally, intelligent DNS services not only allow a service provider to manage its core network like a cloud, making all resources available anywhere and anytime. They also can steer traffic to specific services and VNFs depending on the context of the traffic and the state of the network environment. Subscribers may be directed to certain EPC elements based on the individual subscriber or the application associated with the session. One example might be traffic that is steered to a certain PCRF or OCS, depending on whether the subscriber is a member of a certain family plan for mobile data sharing.

F5 Support for NFV

F5 provides a set of solutions that enable the virtualization, abstraction, scaling, management, and orchestration service providers need to take full advantage of NFV. All F5 services and products are available in virtual models for COTS hardware. Specifically, several F5 data plane and control plane network functions are supported on F5® BIG-IP® virtual editions (VE), all of which can be positioned within segments of NFV-based infrastructures. These functions include virtual services for ADC, IPSECgw, firewall, CGNATgw, SSLgw, DRA/DEA, DNS, and WAF.

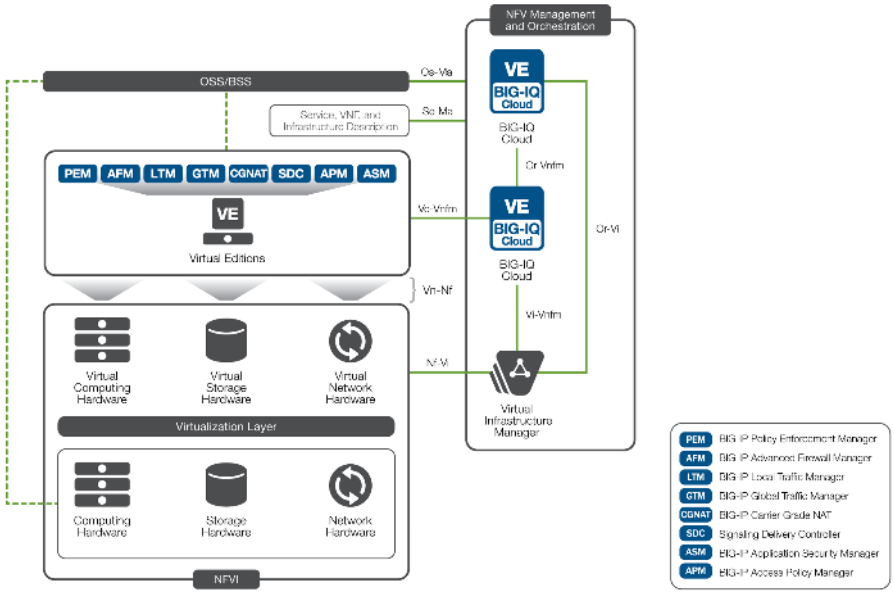


Figure 2: F5 delivers multiple VNF services with management and orchestration.

The F5 NFV solution brings all of these functions together to reside on a unified product platform, the F5® TMOS® operating system. TMOS delivers a common, custom architecture that enables service providers to maximize the benefits of F5 products, which share APIs, real-time features, and functions within today's network infrastructure. The service and management of the TMOS platform is the same whether the solution resides on COTS hardware or F5's custom hardware platform.

F5 also offers a common BIG-IP hardware platform for these services to reside on, bringing together almost all of the described functions. BIG-IP devices optimize performance and functionality for TMOS and any VNFs deployed.

Furthermore, F5 provides technical support to help customers through transition phases of NFV implementation. Service providers buying a BIG-IP appliance today can easily migrate toward a virtualized (VE) network in the future, since both can be managed under the same umbrella and via the same tools. The TMOS foundation is the same across platforms, eliminating functional tradeoffs for operating at required performance levels.

Beyond the available BIG-IP services and products, the F5 BIG-IQ™ platform delivers a network management and orchestration system. BIG-IQ provides an intelligent framework that simplifies the management and optimization of services and applications. BIG-IQ delivers VNF control capabilities to support and manage all F5 services.

One example is the ability to support a pool of licenses for a designated VNF. As virtual instances of the VNF are spun up and down, the licenses can be deployed as needed, minimizing the cost and optimizing the management of software licenses. As a result, it is no longer necessary for service providers to purchase and deploy licenses based on peak scenarios in each physical location.

BIG-IQ can also potentially manage and orchestrate the VNF services in the network. Through open standards such as HTTP/REST and publically available APIs, BIG-IQ can work with existing virtual orchestration engines that manage the virtualization layer of the NFV architecture. This allows service providers to deploy and manage application delivery services in a fast, consistent, and repeatable manner, regardless of the underlying infrastructure.

One Recommended Path Towards NFV

F5 encourages operators to reduce their infrastructure costs through service consolidation while providing them the ability to create new services and revenue models through network agility and application intelligence. These benefits can be realized in a meaningful phased introduction of the NFV architecture.

As NFV gains momentum, this becomes an opportunity to do proof-of-concept trials virtualizing services within the VAS tier. The consolidation and virtualization of services within the S/Gi network associated with the VAS solutions is a natural progression.

Many advanced content- and subscriber-aware services are concurrently implemented in the S/Gi network, creating a complex and hard to manage infrastructure. VAS steering to solutions such as parental controls, video optimization, and security require intelligent dynamic service function chaining that understands the application and subscriber context associated with the data traffic.

Other services such as advanced S/Gi firewall security and IPv6 carrier grade NAT are deployed to help manage, protect, and optimize the S/Gi network. It makes sense that all of these content- and-subscriber aware services leverage a common subscriber and content management technology, such as the F5 BIG-IP platform.

All of these services can be virtualized within a hypervisor framework on COTS hardware. The virtualization of these services and abstraction through ADC and GSLB technologies enables the virtualization of the EPC. Management and orchestration of these virtualized services enables on-demand provisioning of VAS solutions within a cloud-like infrastructure.

After introducing NFV in the services plane, control plane elements, such as the SBC, PCRF, HSS, and IMS services, can be virtualized and brought into the NFV architecture. Orchestration can be extended to take advantage of services within the control plane where the S/Gi elements interact with these backend services through Diameter signaling and SIP messaging.

Finally, the virtualization of the EPC and other core components in the LTE network enables NFV technologies to access key analytical data that leverage dynamic and flexible operator policies to enable the ANI orchestration environment. Operational concerns, such as like network congestion, NFV forwarding graphs, and subscriber and content policy management, can all be managed through the ANI management and orchestration environment. The service provider network is now a truly dynamic, flexible, and automated self-adapting ecosystem.

Conclusion

Service providers deploying in an NFV environment can best realize the technology's promised benefits with F5, whose core competencies with abstraction and ADC-based solutions can help operators build the network of tomorrow today.

Drawing on strengths in service and network abstraction and programmability in the data and management plane, F5 has enabled advanced and automated orchestration systems that equip service providers to react on demand, based on operator policies, in response to operational and business events. All F5 solutions are available as virtual editions for a virtualized environment, making them suitable to an overall NFV strategy, and all F5 service provider solutions are designed to enable a non-disruptive transition from existing network infrastructures to fully integrated and orchestrated NFV network architectures. The resulting automation and orchestration can deliver NFV's expected reliability, scalability, and availability while providing unprecedented agility and extensibility.

[1] Network Functions Virtualisation

[2] ETSI Network Functions Virtualization Architectural Framework

[3] Network Functions Virtualization—Everything Old Is New Again

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com