White Paper

Network Functions Virtualization—Everything Old Is New Again

Service providers are looking to use network functions virtualization (NFV) to build dynamic, virtualized networks with application and content awareness so they can deliver new and innovative services to subscribers, who are changing how they use connectivity services. F5 technologies deliver the necessary application-layer intelligence, orchestration, and policy management to enable effective virtualization and service monetization.

by Frank Yue
Technical Marketing Manager, Service Provider

Contents

Introduction

Communication service providers (CSPs) are facing challenges on multiple fronts. Their traditional sources of revenue, voice and video, are losing ground to services being provided over the top (OTT) on their data channels. At the same time, the infrastructure needed to handle all that data traffic needs to grow to meet the expanding capacity requirements. As a result, infrastructure costs are growing faster than subscriber revenue growth. Operators who try to respond with new ways to monetize their services are realizing that their networks need to become more agile so they can introduce new services more quickly.

In short, CSPs need a new approach to their infrastructures. Yet this need for innovation is not new. The industry has long invented and deployed new technologies to help CSPs offer new and multiple services in a more agile and cost effective way. The difference over time has been at what level in the OSI stack such technology was deployed. Today CSP solutions have reached the application layer, layers 4 through 7. This is new.

With more than a decade of expertise managing L4-L7 traffic and delivering key infrastructure components, F5 Networks enables customers to meet this new challenge. F5 technologies deliver application-layer intelligence with infrastructure virtualization that takes advantage of cost efficiencies, automation, and increased orchestration.

The Service and Infrastructure Evolution

In the past, the primary concern of CSPs was basic connectivity with a single service, which could be voice, video, or data. Their subscribers had similarly single-minded expectations. Operators pulled wire or cable to residences and businesses or set up radio towers to provide this basic, single-service connectivity.

As that connectivity and service became ubiquitous, CSP customers started asking for multiple services such as voice and data or video and data. Initially this doubling of expectations required the creation of a duplicate infrastructure: fixed line operators pulled two wires to a residence or business, one for voice and one for data. This created the infrastructure cost curves we see today, where costs started to outpace revenue or profits, and thus this growth model was determined to be unsustainable. The communications industry created new technologies to help alleviate these infrastructure problems, introducing layer 2 virtualization technologies such as frame relay (FR) and asynchronous transfer mode (ATM). These technologies allowed operators to deliver both voice and data across the same physical (layer 1) medium to preserve a common infrastructure and reduce costs, even though managing the separate voice and data networks in the core required different skill sets.

By the mid 1990’s, customers also were requesting Internet connectivity and IP data services. As the profit margins for basic voice and data connectivity dropped, operators found they could charge a premium for connections to the Internet. This new source of revenue was welcomed, but it also required a new infrastructure that operated at OSI layer 3 and sat on top of existing FR and ATM data infrastructures. Those new networks were funded by the premium that could be charged for Internet access, while customers still paid operators for voice, data, and video services, and the Internet protocol essentially “virtualized” layer 3.

In the early years of the twenty-first century, the Internet continued to disruptively change market and network dynamics. Internet connectivity was becoming ubiquitous, provided by fixed, cable, and mobile operators and differentiated primarily by price. Customers went to the provider with the lowest cost. While traditional voice and data operators started looking to add video services, and traditional video and data companies started to add voice services to compete, further reducing differentiators between them.

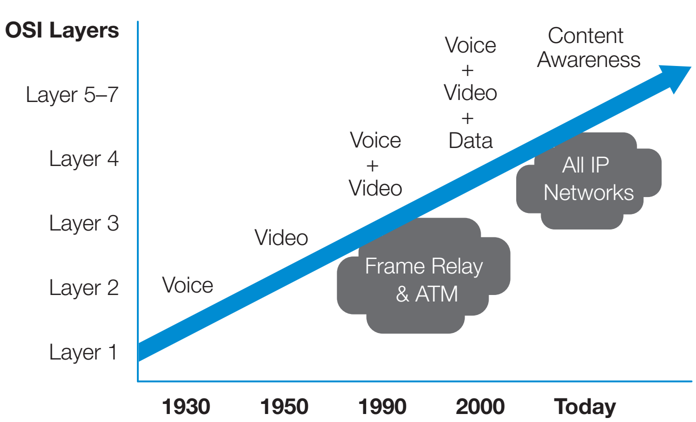

Figure 1: The evolution of CSP infrastructure in response to shifting service demands

The market started to capitalize on CSPs' race-to-the-bottom for the pricing of connectivity. With more voice and video services offered on the Internet, operators saw the need to increase the speed and capacity of their infrastructures to keep up with competitors. At the same time, they were losing their traditional voice and video customer base. Mobile CSPs experienced a similar shift as traditional services such as voice and SMS, which used to generate the bulk of CSP revenue, were replaced by the introduction of smart phones and user migration to Internet-based services. A new generation of customers preferred chat and social networking sites to traditional voice calls. While the benefits of a common IP-based infrastructure had been clear to most CSPs since the turn of the century, they soon came to the realization that the layer 3 IP no longer generated a premium revenue stream but was now an infrastructure component. The real value today is found at higher layers of the OSI model.

Moving up the Stack to Find Value

Today, CSPs are facing another network transition point driven by increasing infrastructure costs, flattening revenues, and the need to provide new services while more efficiently monetizing OTT services on their networks. Reducing network costs and generating new revenue streams both require advanced layer 4 to layer 7 intelligence in the network. This new network needs to be agile, programmable, and adaptable. Enterprises and web-based businesses have been making a similar transition in their data centers, using the advancing cloud computing technologies, for the past 5-plus years.

In the CSP industry, mobile operators are leading the design efforts to monetize services. Mobile networks are built with policies as an essential element of their foundations, since mobile network specifications include the ability to establish and enforce policies within the network. This policy creation and the necessary enforcement take place on services operating at the higher application layers (L4-L7) in the network. This means operators have to become more application and content aware and have the necessary skills to manage a network operating at those layers—including full understanding of the behaviors of TCP/UDP, sessions, and applications, which legacy CSP network and lower-layer forwarding solutions are not built for.

As this new infrastructure incorporating policies is built, infrastructure costs still must be managed with some combination of approaches to reducing capital expenditures and operational costs, optimizing components, and introducing more agility into the network for quicker adaptation to changing market demands.

The Infrastructure of Tomorrow

The leading effort by operators today, called network functions virtualization (NFV), introduces virtualization technologies into the core network to create a more intelligent, more agile service infrastructure.

What is NFV?

According to the Network Functions Virtualization Working Group of the European Telecommunications Standards Institute (ETSI), NFV "aims to address… problems by leveraging standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in datacentres, network nodes and in the end user premises."

The key goals of the NFV Working Group are to:

- Reduce equipment costs and power consumption.
- Improve time to market.
- Enable the availability of multiple applications on a single network appliance with the multi-version and multi-tenancy capabilities.
- Encourage a more dynamic ecosystem through the development and use of software-only solutions.

All of these benefits can be derived from the use of commercial, off-the-shelf (COTS) hardware that can be purposed and repurposed for multiple telecom-related services that currently use proprietary hardware. NFV is taking the software defined networking (SDN) concept of the virtualization movement and adapting it to benefit the telecommunications application infrastructure.

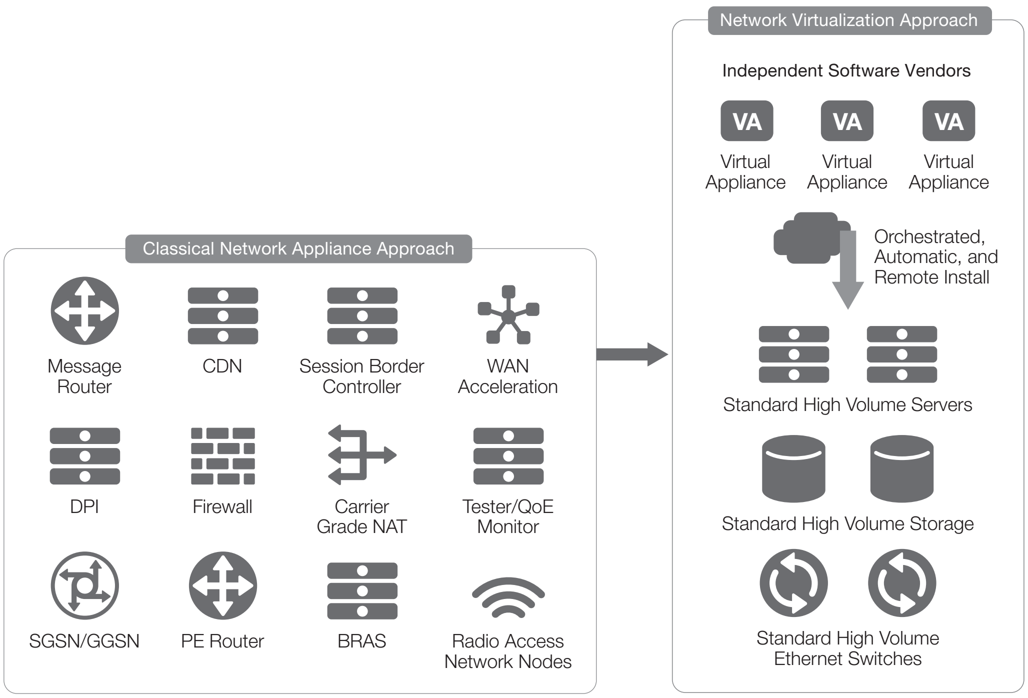

Figure 2: The ETSI vision for NFV, which relies on COTS hardware and software delivered through the cloud

The Benefits of NFV

Virtualization technologies deliver a variety of benefits for CSPs to position them for the next wave of connectivity service and its monetization while also enabling more agile adaptation to future changes.

Lower capital expenditures

COTS hardware is one component CSPs are considering to reduce their CapEx. COTS hardware is typically less expensive than purpose-built, manufacturer-designed hardware. By shifting more components to a common physical infrastructure, operators improve their purchasing power.

Utilizing a common, COTS hardware platform, and thus eliminating specialized hardware for every application onsite, also can help reduce the costs of keeping spare hardware, also known as operational sparing costs. It further enables CSPs to set the stage for virtualizing their infrastructure in a common manner and running services as software. Services can be shifted easily and as needed. COTS hardware eliminates concerns about interoperability or the differences between specific implementations of two different but proprietary vendor solutions.

Lower operational expenditures

Virtualization of the infrastructure streamlines the operational processes and equipment used to manage the network. For instance, an obvious benefit is an improved and simplified model for sparing hardware. Since all the services utilize the same COTS hardware, the CSP no longer needs to support multiple vendors and hardware models, and base hardware support becomes more consistent and easier to manage. Similarly, base software can be unified and more easily supported, with a single unified infrastructure to manage services.

This unified infrastructure also allows for automation and orchestration within and between different services and components. From a single set of management components, administrators can coordinate resource availability and automate the procedures necessary to make services available, reducing the need for human operators to manage the process and reducing the potential for error.

Increased flexibility

NFV using COTS hardware also simplifies the addition of new applications and services as the CSP continues to evolve its business model. New services require minimal training and can be deployed with minimal disruption to the network infrastructure.

Overall, a CSP using COTS hardware can expect broad operational cost savings when virtualizing the network infrastructure and services associated with this new network model. Utilizing a common, agile infrastructure platform enables simplified operational support.

Where and How to Start

As CSPs start to introduce virtualization into their networks, they should approach this network evolution in a pragmatic manner and start by looking at the workloads best suited for virtualization today. Those include services that are CPU or memory intensive on a per connection/user basis and/or those with low network input/output demands. For mobile operators, prime candidates include services located on the Gi LAN, such as video optimization, parental controls, URL filtering, legacy WAP gateways, and other value added services (VAS).

By first tackling virtualization of a small portion of the network, operators can work out all the organizational, support, vendor, and architectural challenges that naturally occur when moving to a new model. These challenges include creating a shared services infrastructure where the Gi LAN services can run.

Organizationally, successful NFV implementations typically include a team that manages the server and hypervisor infrastructure across the services and supports individual VAS solution teams (e.g., a video optimization team, a parental control team, a WAP gateway team, etc.). CSPs also need to work out vendor demarcations and support responsibilities, as a given vendor will no longer bring a combined hardware and software solution but just the software it is responsible for.

Taking this incremental approach enables the CSP to introduce the necessary virtual machine management system and connections to the services infrastructure—in addition to the network infrastructure—to realize operational gains through orchestration and automation. Nonetheless, Gi LAN services or CPU or memory-intensive services are only two of several potential areas where CSPs can introduce NFV. Another could target equipment on customer premises or policy management hardware. The key is for CSPs to pick a discrete introduction point, start small, and use that platform to work out technical challenges as well as the inevitable organizational and support issues.

What F5 Delivers for Network Virtualization

For more than a decade, F5 Networks has been managing application layer (L4-L7) traffic and therefore has long experience helping companies address service creation and infrastructure more comprehensively than most vendors in the IP-based infrastructure world. F5 products are key infrastructure components that enable customers to virtualize their infrastructures in a controlled fashion while taking advantage of the resulting automation and orchestration benefits. F5 application-layer solutions provide the flexibility and functionality required by organizations that need advanced traffic management while delivering the high performance platform to carry out these functions.

A successful NFV implementation demands solutions that support four key characteristics: virtualization, abstraction, programmability, and orchestration. The first requirement is the virtualization of the service. F5 solutions are available either as software on COTS hardware, or, when performance is critical, as software modules for F5® BIG-IP® platform hardware. The F5 technology enables CSPs to deliver multiple services that meet the high performance needs of the Evolved Packet Core (EPC) in a virtualized environment.

Abstraction eliminates any physical or geographical restriction. F5 Application Delivery Controllers (ADCs) and Signaling Delivery Controllers (SDCs) deliver access to the virtualized services through traffic management and traffic steering capabilities. These F5 products use a common hardware platform and common management architecture, enhancing the flexibility that abstraction delivers for multiple traffic management and steering solutions while aligning with the concepts of the NFV Working Group. F5 iApps® Templates further provide administrators with a set of tools that abstracts individual configuration elements into business logic that drives and speeds configuration. Finally, F5 solutions, including BIG-IP® Policy Enforcement Manager™ (PEM) and BIG-IP® Carrier-Grade NAT (CGNAT), also ease management of L4-L7 content, applying context based on operator- and customer-defined policies to steer traffic to multiple services and VAS solutions.

Programmability requires a common and open API toolkit that allows components of the NFV ecosystem to communicate with each other. With the F5 iRules® scripting language, administrators can program and customize the service functions delivered within the software package. The F5 iCall scripting framework delivers an open, programmable management interface. To enable interactions with other components of the virtualized EPC, the F5 iControl® API, which is based on SOAP/XML and REST, provides an interface for communications between disparate systems.

Finally, for a complete and successful NFV environment, orchestration of the data and service availability is critical. Administrators must establish a mechanism to coordinate and control the services within the EPC. This can be achieved through the use of the programmable APIs, abstracted service availability, and the flexibility gained by the service virtualization. The orchestration of these services must be completed with a situational awareness of the data and the control plane in conjunction with operator and customer policies. F5 solutions are integrated with leading orchestration solutions, including VMware, OpenStack, IBM, HP, and BMC. They also can be extended, through F5 management APIs, to incorporate other solutions that are programmable and contextually aware of both the underlying network and higher-level, application-based services. As a result, F5 solutions enable real-time changes to the infrastructure and appropriate services, tying together orchestration engines and dynamic network configuration changes. With an understanding of resource use, availability, and other dynamic parameters, the F5 platform can initiate the addition or removal of service resources to accommodate changing service demands.

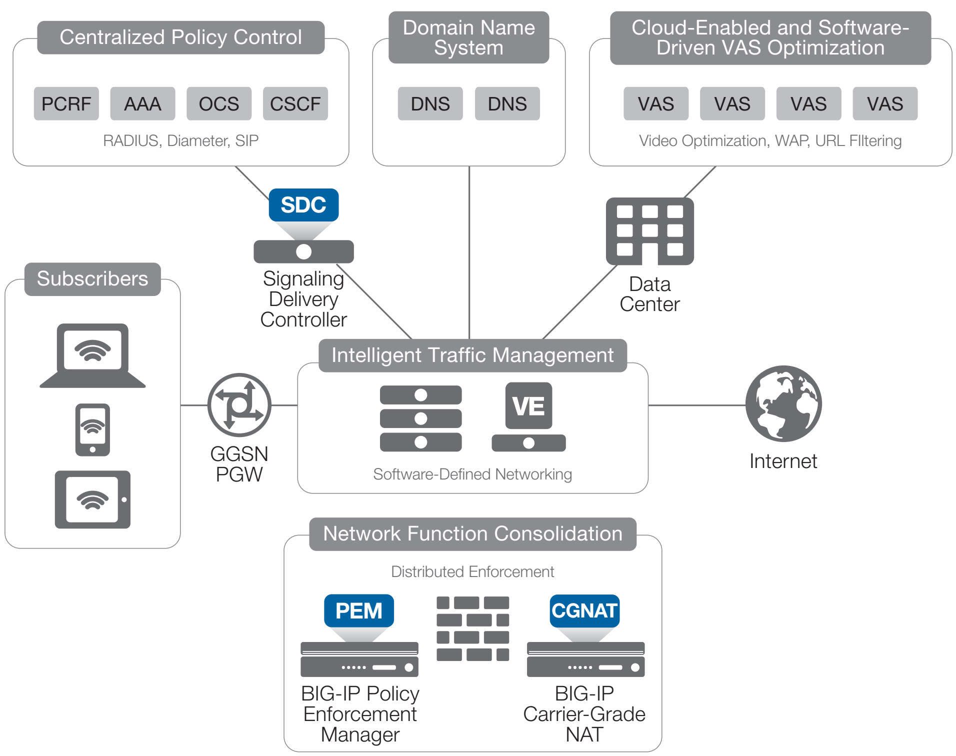

Figure 3: VAS bursting in a virtualized CSP network with F5 products

Conclusion

CSPs are continuing to evolve their networks to meet the changing needs of subscribers, who are moving away from traditional services such as voice and utilizing Internet-based IP services to access increasing volumes of OTT content. To ensure that shifts in subscriber behavior do not make revenue models obsolete, CSPs are adding intelligence to the network infrastructure by adding functionality that moves up the OSI model to application and subscriber L4-L7 content. This intelligence and functionality provides the foundation for new services that generate new revenue streams and deliver additional value to both subscribers and CSPs.

Consequently, CSPs are looking to create a network virtualization framework, such as NFV, to support this new architecture. This framework is centered on the agility to provide services for the subscribers and often incorporates COTS hardware to reduce costs and simplify operational requirements. Technologies that deliver traffic content analysis and policy enforcement are a key part of successful virtualization frameworks.

The F5 platform delivers the necessary application intelligence, content and context awareness, policy application, and abstraction to meet CSP goals and orchestrate the various network and service elements. With F5 technologies and solutions, CSPs can realize their virtualized network goals.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com