Brillio

Brillio
Jan 2022

Table of Contents

Introduction

Connected devices on the Internet which are commonly known as Internet of Things (IoT) are increasing continuously at an alarming pace. There should be adequate network infrastructure facilities to handle the data explosion. One challenge is that IoT devices are globally distributed. The network infrastructure should be able to reach all these globally distributed devices. This is an enormous challenge and a huge investment in infrastructure by any single service provider. Since users are subscribed to many different service providers, and are globally distributed, it is impossible for each service provider to have its own separate network to serve its own subscribers. As new technology emerges, the hardware becomes quickly obsolete leading to huge recurring costs by each service provider.

Challenges for future networks

Technology usage and its forecasted demand is growing at a very rapid phase. To catchup with the demand, research and innovation is continuously providing better and more efficient solutions in the field of data communication networks. These new solutions are essential as previous existing solutions are quickly becoming obsolete. It is not just because we have better understanding of the technology with passing of time, but predominantly because of growing concerns and new requirements. New users are constantly being added to the networks daily as well as new types of network services. Both added number of users and new kinds of services are demanding huge network resources and this demand is growing exponentially.

Concept of network virtualization

First consider the present traditional network scenario. In this scenario, all these different devices are spread throughout the entire network. Since each device has fixed network functionality, the device location has to be carefully planned within the network. After some duration of time, if the network layout has to be changed to accommodate new requirements, these network devices have to be rearranged, reconnected, and then reconfigured individually. Since the control function of each device is embedded into it, each device presents a separate management interface that has to be accessed individually. Sometimes new devices have to be added and the old ones have to be discarded, wasting network infrastructure resources. All these reasons leads to higher infrastructure, operations, and management costs.

Concept Resource provisioning for big data handling

Many experts in industry related to information technology and data networks will immediately conclude that the obvious major sources of data in future would be IoT devices and social networks. When Big Data grows, the concern over its trustworthiness also increases. The data also has to be highly accessible through a simple query mechanism. This is a necessary because the success of any data analysis activity depends on the degree of data availability. If relevant data is readily available, quick and accurate decisions can be drawn from the analytical activity. Decisions based on accurate data analysis will have profound effect on taking sound decisions to improve any business activity. Another major aspect is the speed with which the data can be transferred between relevant users so that they can quickly correlate data to jointly extract and exchange knowledge as well as information. By doing so, they will be able to come up with decisions in time and do not miss any major opportunities. This is crucial for any business to remain ahead of their counterparts.

SDN vs. NFV: Similarities and differences

The core similarity between software-defined networking (SDN) and network functions virtualization (NFV) is that they both use network abstraction. SDN seeks to separate network control functions from network forwarding functions, while NFV seeks to abstract network forwarding and other networking functions from the hardware on which it runs. Thus, both depend heavily on virtualization to enable network design and infrastructure to be abstracted in software and then implemented by underlying software across hardware platforms and devices. When SDN executes on an NFV infrastructure, SDN forwards data packets from one network device to another. At the same time, SDN’s networking control functions for routing, policy definition and applications run in a virtual machine somewhere on the network. Thus, NFV provides basic networking functions, while SDN controls and orchestrates them for specific uses. SDN further allows configuration and behavior to be programmatically defined and modified.

Inside SDN

SDN essentially defines the big-picture side of networking: the kinds of infrastructure desired, the services and applications they deliver, and the network policies that formulate and guide their delivery and use. This kind of functionality – especially the associated rules and policies – changes over time, sometimes rapidly. It also explains the emphasis on programmable network control and the use of SDN controllers with a purview over entire infrastructures. The key ingredients of SDN include the following:

- SDN delivers directly programmable network control: The ability to provision new network elements and devices, or to reconfigure existing ones, comes from a collection of programmable interfaces. This allows administrators to easily program networks either via scripting tools or third-party tools and consoles, all of which employ those programmable interfaces.
- SDN is agile and responsive: SDN permits administrators to adjust network-wide traffic flow dynamically to meet fluctuating needs and demands.
- Network intelligence is logically centralized through SDN controllers: Implemented in software, controllers maintain a coherent global view of the network. To applications and policy engines, SDN looks like a single, logical switch.

NFV explored and explained

NFV, by contrast, is all about the network functions that must be performed at all levels and stages of a network – at the periphery, boundary and core – to accept, forward, shape and filter network traffic as it courses through any given infrastructure.

There are several important points about NFV to note:

- NFV replaces network services provided by dedicated hardware with virtualized software. This means that network services, such as routers, firewalls, load balancers, XML processing and WAN optimization devices, can be replaced with software running on virtual machines. Virtualized network functions are under the control of a hypervisor, which is the role that SDN fulfills in such a scenario.
- NFV helps save both capital expenditures (CAPEX) and operating expenses (OPEX). Network services that used to require specialized, dedicated hardware can run on standard commodity servers (such as ARM, x86 commodity hardware, and so forth), reducing costs. Because server capacity can be increased or reduced through software settings made on demand, it is no longer necessary to overprovision data or service centers to accommodate peak demand.

Where to next?

This is the first in a series of articles on SDN and NFV. The second will explore professional IT certifications that focus on or include substantial coverage of SDN and/or NFV topics. A third piece in this series will share educational resources to help interested IT professionals improve their understanding of SDN and NFV and develop skills in these important topic areas