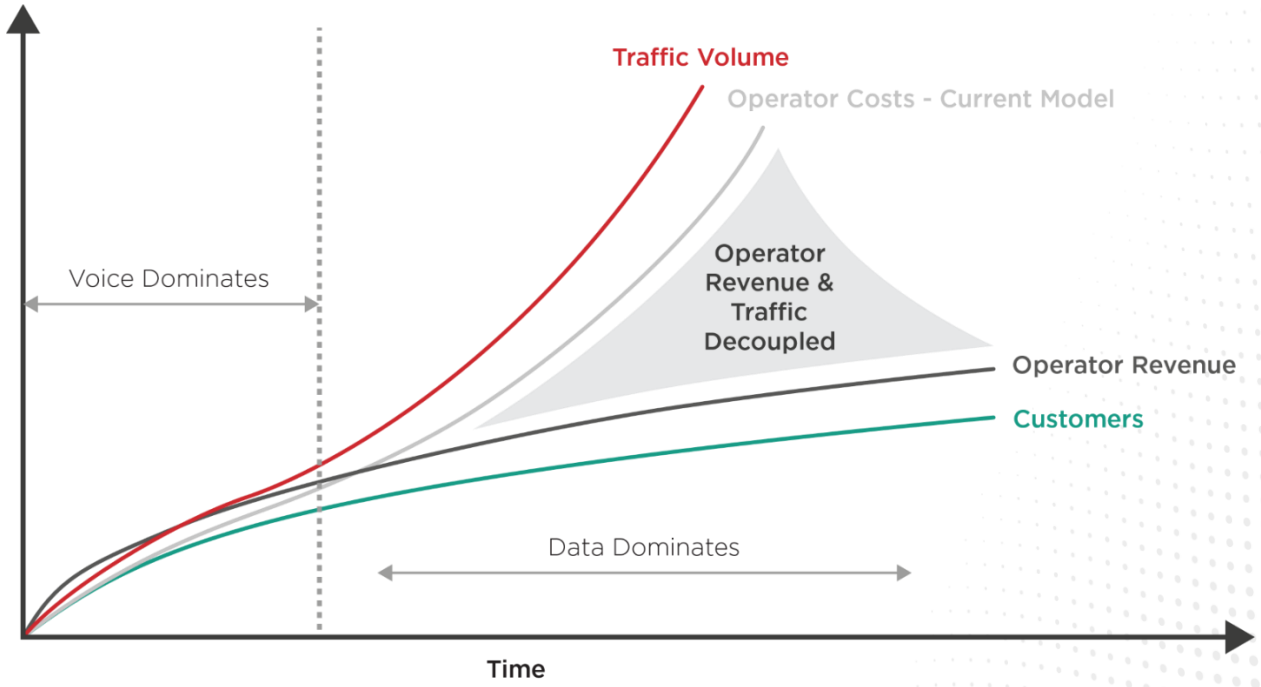
Implementing Software Defined Networks and Virtualisation for More Agile and Scalable Networks

Despite 5G being the most efficient and energy-aware mobile communication standard ever released, the enhanced services provided by 5G—mobile broadband, critical business and emergency communications, massive IoT—will drive traffic volume exponentially.

In the past, service providers addressed these increased network demands by spending more money and buying more hardware. However, network operators cannot allow their infrastructure spending to increase exponentially with network traffic, because the number of customers and the prices they are willing to pay for mobile services will not increase so steeply. Additionally, different data-driven applications have different requirements, so operators need agile, flexible networks that can adapt automatically and in real-time to these different customers.

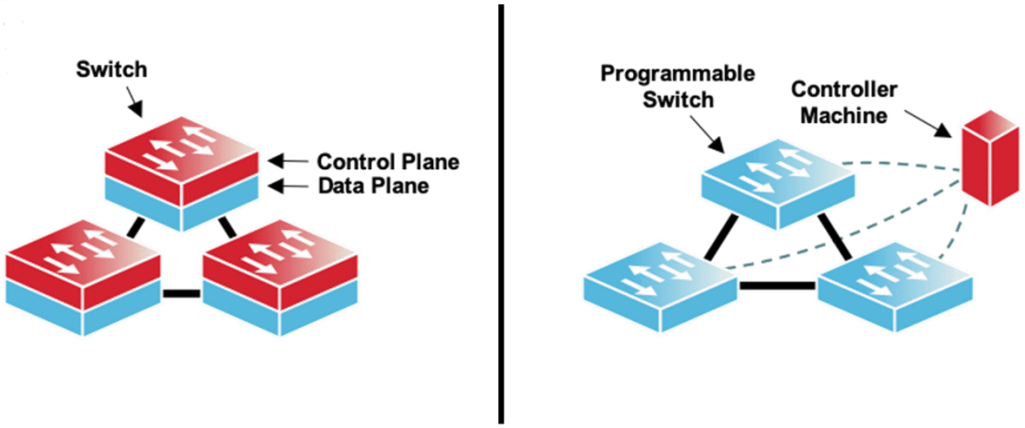


Achieving these joint goals of sustainability and flexibility requires new technologies such as software-defined networking (SDN) and network function virtualisation (NFV).

SDN makes networks more agile and scalable through centralised control

In a traditional network paradigm, switches contained both the hardware that forwards traffic (the data plane) as well as the software that sets the rules of where to forward said traffic (the control plane). Each switch would independently create their routing tables using some kind of network protocol—such as spanning-tree—without receiving much instruction from the rest of the network.

This kind of network would struggle to scale up and be agile enough to meet the increasing demands for bandwidth and new 5G services. To add new types of services and features to the network, each switch has to be configured manually and individually. Furthermore, with data and control plane coupled into the same box, network operators are often constrained by closed and proprietary platforms to interface with the switching hardware.



In a nutshell, the SDN paradigm separates the switching hardware from the software, effectively decoupling the data plane from the control plane. Operators don't have to configure traffic flow rules at each switch anymore but instead can set traffic flow rules at a central controller which will then push these instructions out to the different switches. The language between this controller and the switches is an open protocol, with OpenFlow being the most commonly used one. This guarantees interoperability between switching hardware of different manufacturers and gives operators more freedom to introduce innovative and updated services without being constrained by closed and proprietary platforms.

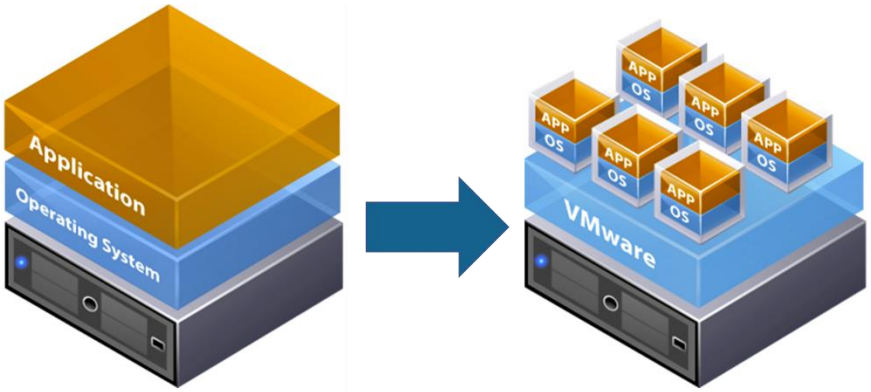
Through the SDN paradigm, business policies can be quickly translated into routing configurations through centralized control. This includes:

- prioritisation (e.g. video traffic over web traffic)
- compliance (isolating finance data from engineering data)
- metering (for service providers)
- reliability (critical applications are configured with higher QoS).

The central controller also has a view of the whole network that individual switches don't have, allowing operators to allocate network resources more intelligently and dynamically. Resources can be allocated through schedules (such as backup services at night) or on-demand (such as adjusting for real-time traffic patterns). This added flexibility and optimisation will improve network outcomes for operators.

Furthermore, SDN improves security by allowing operators to implement different security settings to different types of network traffic. One side of the software-defined network can be used for low-security data that can circulate publicly, and the other side can be used for more sensitive information protected by software-based firewalls and encryption codes. Since the centralised control can see the entire network, end-to-end monitoring and intruder detection can be implemented more effectively, too.

NFV Separates Software From Hardware



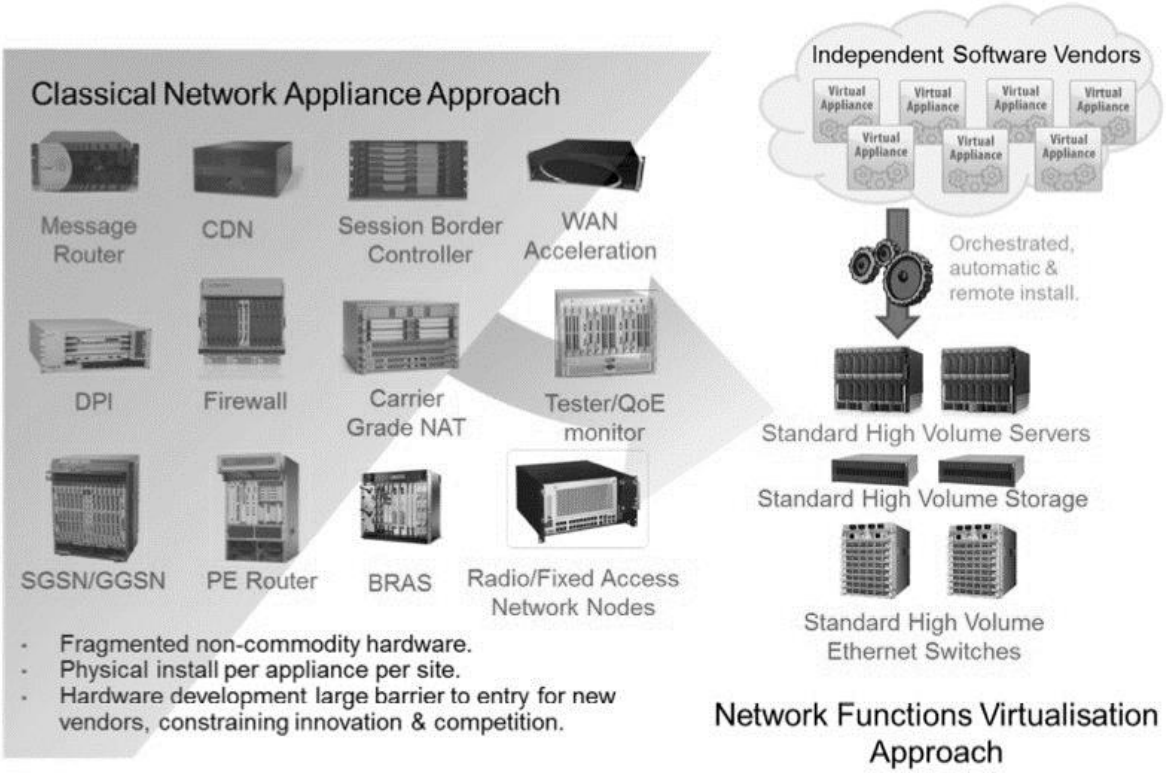
Traditional Architecture Virtual Architecture

Virtualisation technology uses a software emulator (known as a hypervisor) to create an abstraction layer over the physical hardware. In doing so, it creates a virtual computing system known as a virtual machine (VM). This virtualization process effectively separates software from hardware. By partitioning a single unit of hardware into multiple virtual systems, users can run multiple applications that would have normally required multiple units of hardware. Simply put, virtualisation allows for more efficient use of physical computer hardware. After many years of providing increased returns on hardware investment in the IT world, network operators have taken notice, and are now trying to use virtualisation software to run multiple network functions on a single server.

The highly fragmented classical network appliance approach required several specialised hardware units, including routers, controllers, packet sniffers, firewalls. Every time a site needed a new network function, a new appliance had to be installed physically on-site. This kind of hardware development constituted a large entry barrier for new vendors, which hindered healthy competition and quick innovation cycles.

On the other hand, network function virtualisation (NFV) infrastructure consists of commercial off-the-shelf (COTS) servers, storage and ethernet switches. Thanks to the virtualisation layer the same general-purpose hardware unit can implement many different specialised functions, from load balancers to firewalls to VPNs. Since the NFV implementation does not require the installation of new specialised hardware on-site, it can be completed automatically and remotely.

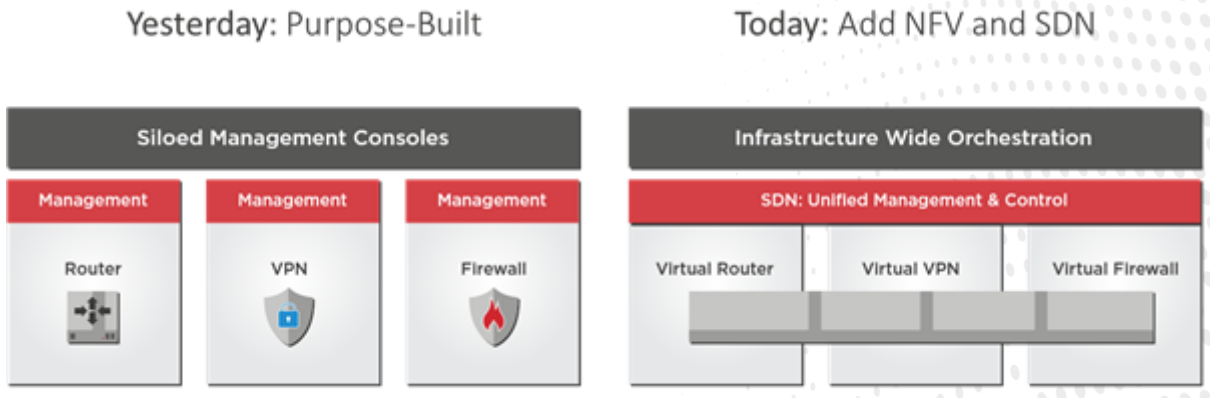
This approach reduces both capital and operational costs. The commercial off-the-shelf devices are produced on a much larger scale than dedicated network hardware, so they are more easily and cheaply procured. Meanwhile, automated and remote installation can deploy new services and applications to users more quickly. By migrating workloads and powering down unused software, operators can also reduce their energy costs. Meanwhile, the standard and open interfaces that control NFV infrastructure help operators avoid vendor lock-ins and thus enable greater flexibility in network implementation, upgrades, and innovation.



Combining SDN and NFV for automation and orchestration

SDN and NFV have a lot of points in common: they both employ some degree of network abstraction to implement network functions and services via software, they use COTS hardware over dedicated proprietary hardware, and they interface with hardware using open APIs for more efficient implementation and automation.

These approaches can be implemented independently, but they synergise well with one another and can thus be combined to provide more efficient and enhanced performance results depending upon what an operator wants to accomplish. SDN is a bit different from NFV but many NFV architectures employ SDN controllers as part of their network. These differences between both the technologies allow them to be implemented together on the same network in a mutually beneficial manner which will enhance the network performance more as compared to the performance achieved by implementing a single technology.



When SDN is employed on an NFV infrastructure, its function is to transmit data packets from one device to another. At the same time, the networking functions of SDN for routing, policy-making and application run in a virtual machine located somewhere on the network. Hence, NFV offers basic networking functions, whereas SDN controls and manages them for specific purposes. SDN also defines and modifies the configuration and behaviour programmatically.

By combining SDN and NFC, operators can create a more flexible and programmable network architecture that uses network resources efficiently. The open standards allow easy access to all information across multiple vendor platforms based on COTS equipment, with no need to get into each proprietary management console as before. This approach provides full visibility across the entire network stack, including options to reconfigure on demand.

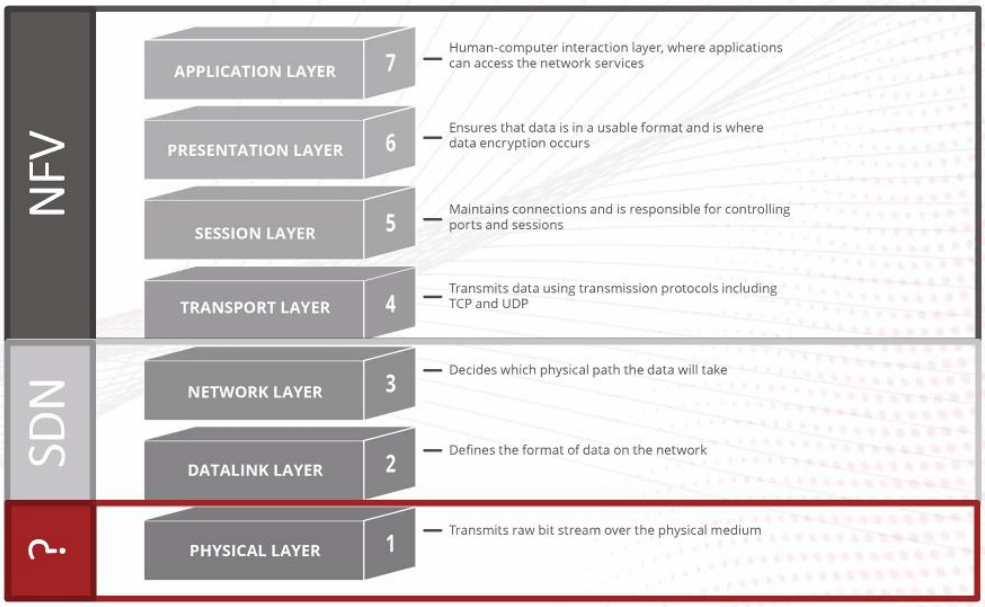
Towards a self-managed, zero-touch automated network

The upcoming 5G networks will consist of a massive number of devices, software applications and technologies. These technologies will occupy large frequency bands that must be utilised efficiently to accommodate the increasing number of users.

Delivering these services with efficiency and sustainability requires the deployment and implementation of SDN and NFV technologies that will simplify the way operators control and manage the network functions with reduced cost and efficient resource utilisation. SDN will give operators more control of the flow of data throughout the network, allowing for a more agile, controllable and secure network later. NFV will give the network operators tools to make more efficient use of their installed hardware base.

However, EFFECT Photonics' vision of the next-generation mobile networks goes beyond SDN and NFV. Ultimately, we want a self-managed, zero-touch automated network. Achieving this full automation requires two additional components alongside SDN and NFV:

- Artificial intelligence and machine learning algorithms for full automation of the network
- Sensor and control data flow across all layers of the OSI model, including the physical layer



NFV unlocks automation and reconfigurability across the top layers (4-7) of the OSI model, while SDN unlocks them in layers 2 and 3, but the physical layer should also communicate with the rest of the OSI stack and be programmable.

In the next article, we will explain how integrated photonics and specifically our DWDM system-on-chip technology can unlock the physical layer to automation and complete the paradigm shift towards fully automated networks.

For more on our optical system-on-a-chip products, visit: https://effectphotonics.com/product/

Contact information

e-mail: sales@effectphotonics.com
phone: +31 403041359
website: www.effectphotonics.com