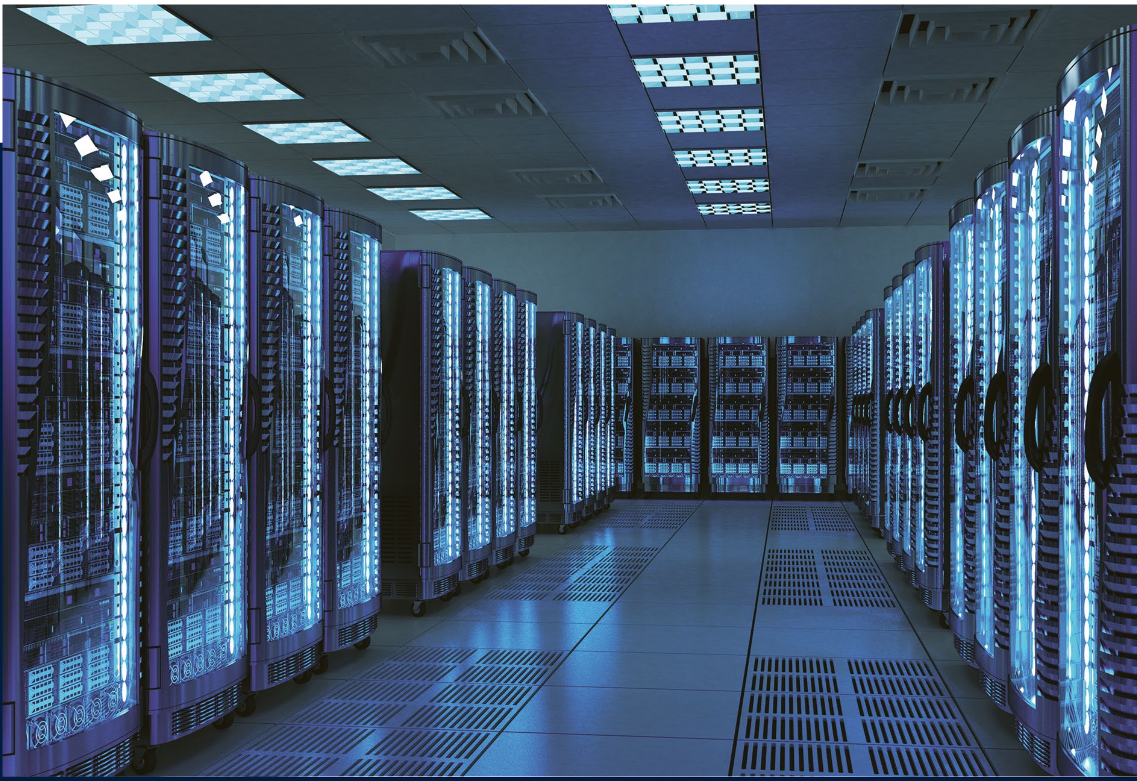
White Paper

NFV – Network Functions Virtualization



The concept of virtualizing network functions is actually nothing new. Manufacturers of network components have for years been using functions such as virtual routing and virtual LAN (VLAN) to logically separate the internal networks of a company, for instance.

A new trend under the supervision of the ETSI Industry Specification Group (ISG) is Network Functions Virtualization (NFV). The aim is to host yet more network functions on generic virtual machines (VM) instead of using specialized dedicated hardware, as in the past. The devices in question include routers, firewalls, and load balancers.

The aim of NFV is for software-based equivalents to replace hardware-based features such as virtual private networks (VPNs), security features such as firewalls and session border controllers, and gateway features such as routing VLANs.

This white paper highlights the key benefits of NFV and uses the example of replacing hardware routers with software-based routers.

Advantages of NFV

Companies save money by using NFV for certain applications within their overall digital transformation of processes.

Investment in hardware that fulfills a single fixed purpose is reduced. Comparatively low-priced, standardized industrial servers are used instead, and they support multiple virtual machines to operate these functions. What's more, the simplified rollout and management of network services further reduce the operating costs.

But cost reductions are not the only benefit. NFV generally supports what are referred to as "pay as you grow" solutions. This enables the services to respond dynamically to a company's growth, which makes them extremely future-proof and efficient.

Similarly, this accelerates the processes involved in deploying new network services to meet changing business needs, exploit new market opportunities, or simply accelerate ROI by introducing new services. When it comes to changing requirements, NFV helps to adapt quickly by scaling capacities up or down accordingly. Consequently, virtual network devices are usually more flexible and agile than traditional hardware-based services.

Another interesting aspect is that NFV is based on virtual appliances. Virtual appliances are preinstalled, preconfigured, out-of-the-box applications, and software solutions that are bundled with an operating system on the virtual machine. Technical innovations are supported more quickly because virtual appliances can run on any server at short notice. Thanks to the regular updates and the corresponding hypervisor functions, virtual appliances run extremely reliably and failsafe.

Another effect is that the risk of testing new features is minimized, as is the time required to introduce new services.

Virtual routers

So virtual routing was created as a type of NFV, where the functions of hardware-based network routers or gateways are implemented in software. This software runs on off-the-shelf industrial servers with the usual advantages, including low cost and increased interoperability. Instead of a proprietary hardware platform, the company IT gets a familiar system.

This is crucial for companies with branches in several countries, for instance. They benefit from a centralized rollout and the immediate availability of software-based networking capabilities. No waiting for the network hardware to be ordered, shipped, installed and configured by local IT experts. Local branch offices need the presence of network administrators less often, which reduces travel expenses. At the same time, this enables more flexible processes and faster reaction times to changing requirements.

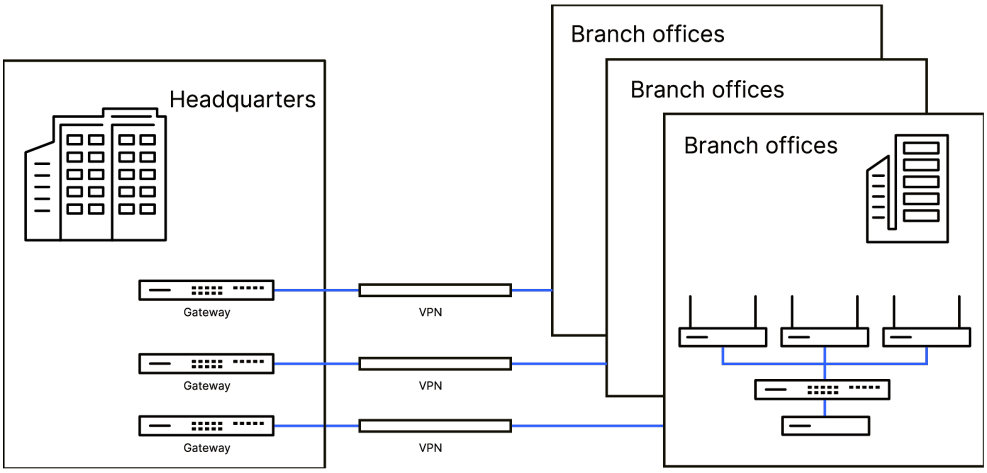


Figure 1:
Classic infrastructure

A virtual router is an application that replicates the functionality of hardware-based Internet protocol (IP) routing. So far, this has always been dedicated hardware. Virtual routing frees IP routing from this dedicated hardware and allows the functions to move freely to a data center. What's more, these virtual functions can be set up dynamically, automatically, and in accordance with individual requirements.

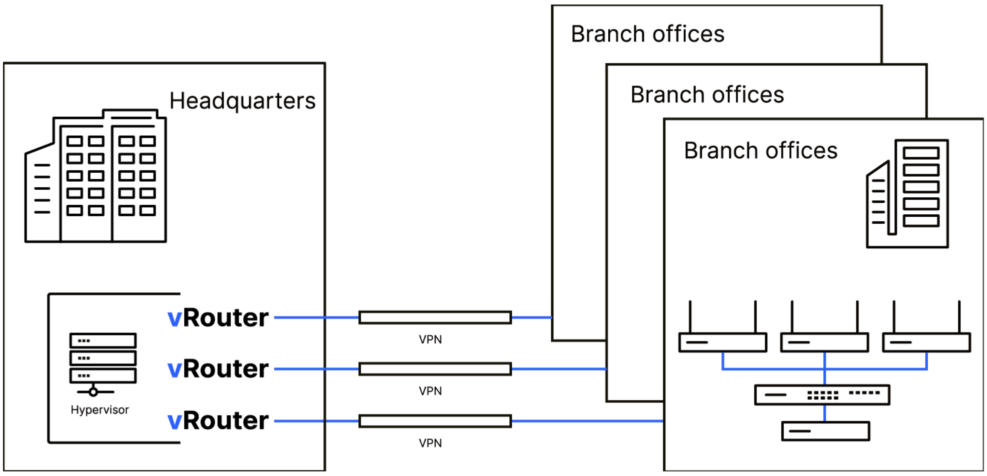


Figure 2:
Virtual infrastructure

Another highly interesting aspect is the ever-increasing demand for cloud-based services that are added at the click of a mouse—without a time-consuming start-up phase or the commitment of your in-house IT resources. Virtual routers are the ideal, secure connection between enterprise networks and public cloud offerings such as Microsoft Azure or Amazon Web Services. You „extend" your own secure network to encompass the cloud services, which effectively prevents any compromise of the data transmission paths.

Is a real router always the best solution?

The virtualization of network functions is not a new development or trend in the world of IT. For years already, device manufacturers have been using virtual routing capabilities to map complex VPN scenarios and VLANs within their VPN gateways and routers.

A virtual router provides the maximum performance of the underlying virtualization platform. As a consequence, it can provide significantly more IPSec VPN tunnels than a real router. The response to increasing demands is simply to upgrade to faster server hardware and for the hypervisor to move the virtual router, a process that is completely transparent and without any significant loss of time. These aspects make the virtual router highly attractive as a central-site router / VPN gateway for networks of any size.

It is therefore a secure endpoint for secure VPN tunnels in cloud projects and offers highly automated configurations based on SD-WAN.

The consequence is that a virtual router is the best solution for a wide range of scenarios. However, there are still scenarios where hardware-based routers are the better option. Hardware is indispensable if, for example, there is a physical connection to the Internet via DSL or fiber-optic lines. In practice the structures are often hybrids, with hardware-based local routers at branch offices using VPNs over various Internet connections to connect to the virtualized VPN gateway.

Summary

NFV is the next step in the virtualization of enterprise IT infrastructures. The flexible scalability of these solutions offers a level of future-proofing that so far could not be achieved with hardware.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com