Technology Advancements at the Speed of Safety

Paul Groppel

Sean Bowden

NFV

The impact of technology maturity on a mission-critical network can be illustrated through SDN and NFV capabilities. SDNs grew from the need to offer more network flexibility without the increased costs of operating and maintaining a large network infrastructure. Like SDN, NFV was developed to reduce costs and accelerate service development for network operators.

Where SDN decouples routing control from network devices, NFV decouples network functions from dedicated hardware and moves these functions to virtual appliances. It removes the need to purchase expensive, proprietary hardware that provides a unique function like routing, encryption, firewalls and load balancing. Instead it enables the ability to move these functions to less expensive devices that support virtualization. Virtualization reduces dependency on dedicated hardware appliances and allows for improved scalability and customization across the entire network.[1] NFV is also designed to reduce the manual effort of maintaining network devices by automating the application of standard configurations to devices. This reduces the impact of accidental misconfigurations caused by manual device management.

While NFV offers significant value and cost savings it also has its challenges. In traditional networks, proprietary hardware such as routers and switches are often designed as dedicated appliances with built-in failure protections or hardware configurations specifically to meet network traffic loads. In an NFV environment however, more generic components are used which may not be able to support throughput challenges. In addition, NFV software packages may contain open-source code or solutions which can add to the complexity of building a standardized and scalable infrastructure. This can lead to inconsistent architectures that can negatively impact network service offerings.

To address these challenges, organizations can leverage NFV solutions that have a standard baseline of hardware and software components that have been validated by industry and meet basic compliance standards. NFV solutions should be interoperable with legacy h

To reduce costs, cellular wireless providers share their transport with multiple customers in the public sector. While there are efforts underway for private 5G backbones, these solutions still share resources with a limited customer set and cause challenges with prioritization. While the promise of higher bandwidth over the airwaves sounds like a great option for data paths, limiting the use of cellular wireless to non-critical services is a prudent approach. LTE has latency and jitter issues which is problematic when critical services may require extremely low tolerances to both. Leveraging SD-WAN can aid in boosting network and application performance to minimize these impacts.

Another challenge to consider when looking to adopt an LTE network is that cellular data is exposed to cyber threats. They can be directed towards exploiting or impacting radio frequency (RF) communication paths. A denial of service of wireless devices and networks is also possible. Saturating the device with RF noise, or jamming, could severely degrade a RF signal and in some cases, cause a device to shut down. In this example, technologies like SD-WAN are configured to recognize communication path interruptions and can often re-route traffic seamlessly and avoid the impacted link.

For commercial use, LTE might be a viable access solution to reach the masses and provide voice and data services, but for life-critical applications