WHITE PAPER

Communications Service Providers
Cloud-Native Network Functions

Evaluating and Integrating Cloud-Native Network Functions

Learn what to look for when selecting cloud-native network functions (CNFs) for the 5G core network, and best practices for testing and integrating them into the network

Authors

Richard Band
Head of Mobile Core and 5G,
Hewlett Packard Enterprise (HPE)

Petar Torre
Principal Engineer,
Intel

Table of Contents

Hewlett Packard Enterprise

Executive Overview

The advent of 5G is a game-changer for communications service providers (CoSPs), offering exciting opportunities for new services and customers. But 5G also poses some challenges for CoSPs. For example, 5G demands that the core network be cloud-ready, resilient, and agile. Legacy technology and long-standing procurement and deployment strategies will not work in a 5G world.

As CoSPs begin to explore building a 5G core network, they will need to incorporate cloud-native network functions (CNFs). The industry is moving too fast to continue with existing product development and deployment practices. Those CoSPs who adapt to new deployment frameworks will have a competitive edge. But how do CoSPs go about evaluating network functions offered by independent software vendors (ISVs) or other firms? How do they test and integrate these new cloud-native functions? What new skills do CoSP personnel need? Hewlett Packard Enterprise (HPE) and Intel specialists answer these questions in this white paper. They share industry expertise that CoSPs can use to advance their 5G core network deployment.

Business Challenge

Historically, communications network upgrades have required months, or even a year to complete. That pace won't work for 5G. By its very nature, 5G requires the core network to be agile and configurable, driven by CNFs. As new use cases arise, network slicing can be used to bundle the appropriate CNFs and provide services. But the market moves fast—CoSPs need to quickly select which CNFs to deploy. Then they need to test them and get the service up and running in a matter of a couple months maximum. This is a far more dynamic environment than some CoSPs are accustomed to. To survive—let alone thrive—they need a different strategy that lets them speedily monetize the network.

Beyond business agility, another challenge is to lower total cost of ownership across the core network. Traditional vertically integrated silos drive up costs, as do manual, high-touch maintenance and upgrade processes. CoSPs need to move toward using more open source tools that can lower development and deployment costs. As the lines between telecommunications and IT blur, increasing adoption of IT-like automation tools can create cost efficiencies. But these are uncharted waters for most CoSPs, who may lack IT skills and who may be unsure of where to start.

Adopting a New Procurement and Deployment Strategy

While deploying a 5G network does require some new technologies and skills, the biggest adjustment for CoSPs will be changing how they procure network components. Traditionally, CoSPs around the world have had a relatively small number of suppliers to choose from. They have taken one of two procurement/deployment approaches (see the first and second columns in Figure 1):

- **Single-supplier.** The entire core network runs on one supplier's technology stack and the supplier takes responsibility for core network functionality. While this approach can simplify things, it also raises issues with vendor lock-in and limited opportunity to adopt new technology as it becomes available.
- **Best-of-breed selection.** The CoSP constructs the network itself (virtual network functions (VNFs), servers, storage, and more) usually with help of pure-play system integrators. Suppliers are selected based on their ability to do specific functions. The CoSP performs function integration in-house. While this approach avoids vendor lock-in, it takes a lot of in-house skills. It also can be time-consuming—and will only get more complex as additional suppliers come on the scene with new CNFs.

The industry is evolving to include a third "mixed/hybrid" option (see the third column in Figure 1) that better accommodates cloud-native 5G core network requirements. For example, many ISVs are replacing their proprietary, non-differentiating service components with open source Cloud Native Computing Foundation (CNCF) projects. Examples of such components include logging, tracing, telemetry, registries, and databases. These CNFs will all use a common platform services framework. CoSPs will be able to more easily integrate components from different suppliers. Alternatively, they can work with a system integrator to select the right CNFs from the right suppliers and perform pre-integration. The end result will seem more like the single-supplier approach, with less risk of vendor lock-in.

Evaluating Cloud-Native Network Functions

A few years ago, CoSPs and vendors made large investments to transition from physical network functions to VNFs. This move helped CoSPs achieve gains in both cost efficiency, because of the volume of IT equipment, and agility in software.[1] But technology never stands still. As wide-spread deployment of 5G looms closer, it's time for CoSPs to again adapt—or risk being left behind by more agile providers. Rather than replacing existing VNFs, the move to CNFs means implementing a service-based architecture (SBA). This architecture uses new functions that are specifically designed for the 5G core network.

Conservative	Disruptive	Mixed/Hybrid
Gradual evolution of existing network keeping existing processes and suppliers	Do It Yourself using in house capabilities and combining best of breed components	Use a pre-integrated stack built from proven cloud-native components and standard aligned functions
+ Limited technical and financial risks + Single point of accountability + Limited impact on processes and methodologies	+ Full control + Avoid vendor lock-in	+ Limited technical and financial risks + Avoid vendor lock-in + Leverage partner's know-how
- Limited options - Risk of vendor lock-in - Slower innovation	- Need massive in-house skills - High technical and financial risks - Can lead to a proprietary solution	- No smooth migration from existing network - Requires evolution of processes and methodologies

Figure 1. Communications service providers (CoSPs) can avoid vendor lock-in and complexity by working with a system integrator to build a standards-based 5G core network.

But as the number of suppliers of CNFs proliferates, what should a CoSP look for? In a nutshell, a true CNF will be decomposed into containerized microservices, use immutable infrastructure and declarative application programming interfaces (APIs). Other things to check for include the following:

- To what degree a network function is cloud native:
  - Is it decoupled from the underlying infrastructure and platform services?
  - Is it resilient to full failures and impairments? (more on this in the next section on testing)
- Can it support five-nines service quality, and is CNF availability configurable at deployment time?
- Can decomposed components be upgraded separately?
- Are existing components patched/upgraded or is the supplier always rolling out new ones?
- Does it support stateless processing and desired observability?

Once a CNF is selected, it's time to test it, then integrate it into the network.

Testing and Integration

Beyond testing individual CNFs (discussed in the next section), the move to a cloud-native 5G core network involves quite a bit of up-front work that must precede CNF testing. This effort involves establishing a continuous integration/continuous delivery (CI/CD) and automation pipeline, and preparing for smaller, incremental upgrades using canary testing and rolling upgrades. And then there are all the normal activities such as defining specifications, creating hand-over documentation, and installing and configuring software. In fact, the scope and method for testing is very different with cloud native than for legacy non-cloud-native core networks.

Because CoSPs are just getting started with new ideas such as CI/CD and automation, the first cloud-native projects will take more time. This is because there is a steep learning curve for both CoSPs and suppliers. While the external core network integration points are fully standardized, the IT integration is less standardized. But once the IT integration is done, it won't change from one release to another. Therefore, the major business benefit comes post-initial deployment, through acceleration.

Before testing CNF functionality and performance, the underlying platform also needs to be tested for functionality and required performance. For example, the network function virtualization infrastructure (NFVI) must be able to support the packet processing rate that is required by future CNFs.

Testing CNFS

CoSPs can expect to spend one to two weeks testing functional compatibility between telco-specific CNFs. Besides functional compatibility, CoSPs should test that there is no loss of session data in the event of a failure (CNF is stateless). This is an essential component of being cloud native. To test this characteristic, shut down one of the co-processing engines and make sure the other instances are taking over, using session state from shared storage.

One methodology for testing anything new is called "canary testing". It works as follows: A new version of a service is pushed into production and is tested by a small number of end users. These end users verify that the new functionality works as intended and does not cause problems with other services. To perform canary testing, the network must provide independent lifecycle management per microservice. For example, canary testing in the Session Management Function (SMF) runs two versions of the SMF simultaneously while the User Plane Function (UPF) stays the same. More advanced testing includes CNF resilience testing to check if the CNFs were designed to run on a shared cloud platform and are resilient to infrastructure impairments.

CoSPs can take advantage of open communities that are collaborating on defining requirements, methodology and tools for the Kubernetes platform and CNF testing. Examples include the Common NFVI Telco Taskforce (CNTT), which has defined a reference architecture and conformance specifications for Kubernetes, and the CNCF CNF Testbed.

Integration Using Blueprints

The key to success when deploying CNFs is to do the integration correctly—that is, up front instead of on customer premises (the latter would be too costly). CoSPs gain the operational efficiencies of the cloud, but the deployment works like a single-supplier network. HPE and Intel for cloud-native 5G deployments can provide core and edge infrastructure blueprints. These blueprints define high-performance top-of-rack networking, control, storage, and compute nodes. The blueprints use HPE ProLiant, HPE Synergy or HPE Edgeline servers. These servers are equipped with Intel® Xeon® Scalable processors, Intel® Ethernet, Intel® FPGA Programmable Acceleration Cards and Intel® SSD Data Center Family.

Investing in New Skills for the Cloud-Native World

In the past, the world of telecommunications and the world of IT were distinct, with entirely different skill sets. But as CoSPs begin to deploy cloud-native 5G CNFs, they will need to augment their existing skills with IT abilities, including:

- Familiarity with Kubernetes and other key CNCF projects like the Container Networking Interface (CNI), Multus, Envoy, Etcd, Helm and Prometheus
- Ability to deliver CI/CD and automated deployments
- Knowledge of new security and isolation operational paradigms and technologies
- Ability to manage a mix of physical, virtualized, and containerized network functions

Cloud-Native Network Function Best Practices

- Prioritize projects and products where design principles focus on interoperability and open communities. This minimizes the required amount of custom integration to drive down cost.
- Have a sourcing strategy for platform as a service (PaaS). This is foundational for everything else. It also avoids the fragmentation that can occur if several vendors are selected for the same functionality.
- Start with automation from day one. Waiting just makes the hurdles seem bigger and reduces the time available to surmount them.

Conclusion

CNFs are key to building a successful 5G network, but they require some substantial changes to how CoSPs have typically developed and deployed new services. CoSPs are focusing on agility and fast time to market. This is leading many CoSPs to explore more open source solutions and a wider ecosystem of suppliers than in years past. Industry leadership from HPE and Intel can help CoSPs better understand what makes a network function cloud native.

Learn More

- **5G Core Sourcing Strategies:** Openness with Risk Aversion white paper
- **5G Core - Heart of the transformation:** 5G and the IT-ification of Telecommunications webinar
- **Intel Containers Experience Kits:**
  - The "Container Bare Metal for 2nd Generation Intel® Xeon® Scalable Processor Reference Architecture" provides instructions on how to build an open source Kubernetes bare metal environment optimized for data plane CNFs
  - "Packet pROcessing eXecution Engine (PROX) - Performance Characterization for NFVI User Guide" describes testing platforms for CNFs, as well as methodology and tools that Intel has contributed to relevant communities
- **HPE:** 5G Solutions across Telco and Enterprise

They can also help CoSPs develop a skill set for quickly testing and integrating CNFs into the network—driving up those CoSPs' competitive advantage.

Contact your Intel representative or visit **Intel.com/network** for more information.

[1] https://www.informationweek.com/network-virtualization-optimizing-agility-performance-and-cost/v/d-id/1331761

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

0720/FP/CAT/PDF 343126-001EN