NEXT-GENERATION CENTRAL OFFICE (NGCO)

WHITE PAPER

Next-Generation Central Office (NGCO)

Software-defined networking (SDN), network functions virtualization (NFV), and the imminent arrival of early 5G architectures are driving change in communications service provider (CoSP) networks. The telecom industry is embracing new technologies and techniques to drive fundamental change in the way carriers plan, deploy, and manage their infrastructure. This transformation is likely to occur at the aggregation edge, also known as the central office (CO).

One such emerging transformational force is the ongoing upgrade of broadband wireline infrastructure in which CoSPs are continuing to roll out fiber optic cable in fiber-to-the-home or -curb (FTTH/FTTC) deployments. As a result, legacy copper central COs are “melting”—that is, being replaced by fiber-fed COs primarily based on passive optical network (PON) technologies. These deployments have a much longer reach on fiber than was previously possible on legacy copper based COs, allowing the customer base to be served by next generation CO facilities, and thus, reducing the number of distributed COs needed to support a given population.

Key Characteristics in Evolving Telecom Architecture

Figure 1 illustrates a distributed telecom architecture that brings key virtual network functions (VNFs), such as optical line terminal (OLT), customer-premises equipment (CPE), and broadband network gateway (BNG), to the edge. The level of distribution will vary depending on the services supported by the operator. The current trend is for mobile infrastructure to distribute VNFs to mid-mile sites in order to serve the high traffic growth expected in the coming years. For very low latency applications, the mobile user plane will distribute right out to the last mile site or even closer to the base station itself.

From the perspective of Intel and Quanta Cloud Technology* (QCT), next-generation central office (NGCO) architecture will run on the hardware and software offered by ecosystem vendors. An example of NCGO architecture is shown in Figure 2. It allows QCT to integrate a large number of commercial-level VNFs into an edge NFV infrastructure (NFVI) that provides a realizable blueprint for carrier-grade, edge NFV. By adopting this solution, operators can avoid using purpose-built equipment, can reduce their time-to-market and development costs by using x86-based infrastructure that provides a level of integration and build out validation.

The NGCO architecture introduced in this whitepaper can be briefly summarized as follows:

1. Unified NFVI, based on OpenStack* Queens.
2. Network function workload implementation

- Fixed-line and mobile network convergence in one NGCO edge rack
- Security workloads

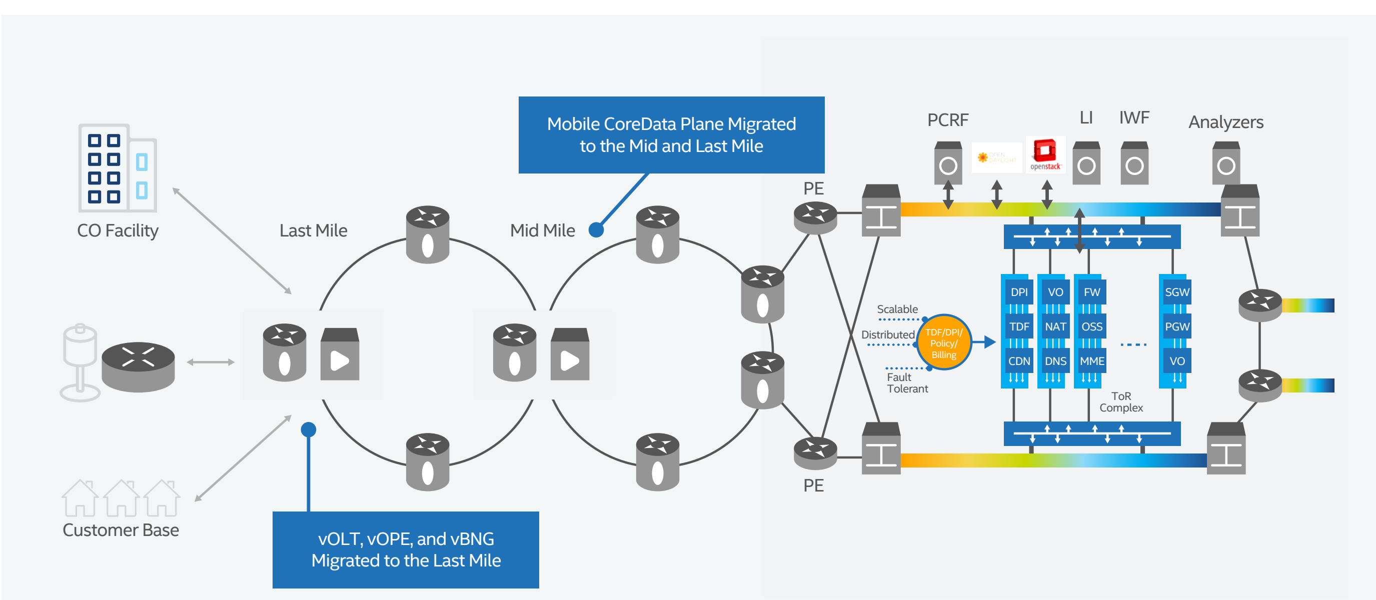


Figure 1. Evolution of Telecom Architecture

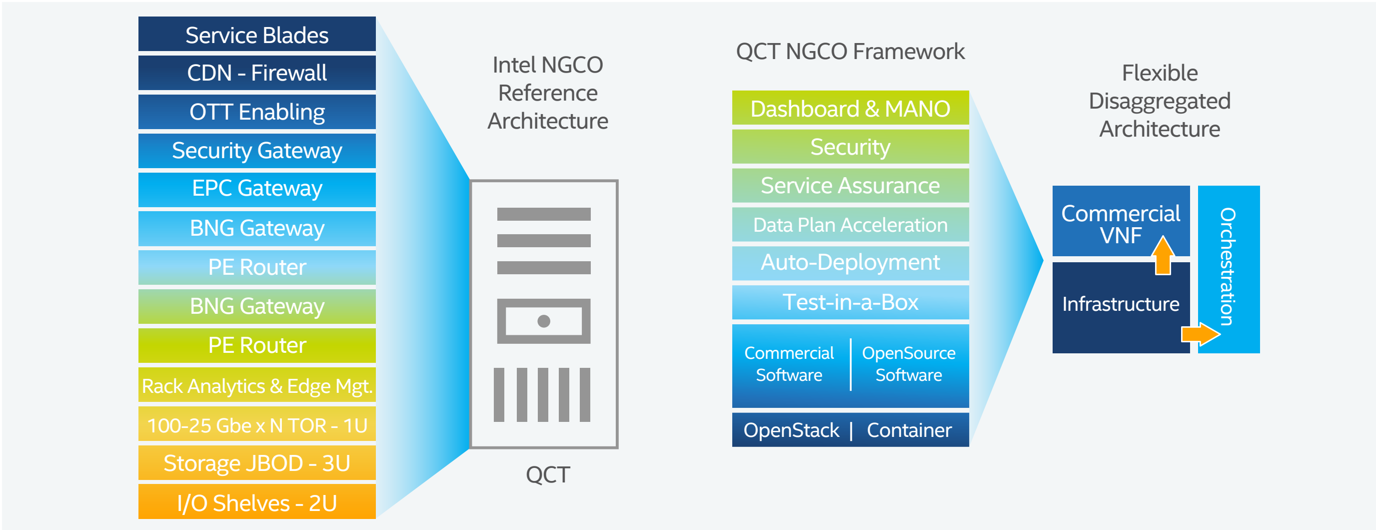


Figure 2. QCT* Next-Generation Central Office (NGCO) Framework

- Edge application workload is deployed by instantiating a virtualized, distributed content delivery network (CDN)

3. Open-source telemetry enabling platform service assurance and closed-loop network automation
4. Orchestration of the NGCO

Network Functions Virtualization Infrastructure (NFVI)

QCT QxStack* Network Function Virtualization (NFV) Infrastructure, on OpenStack* platform("the NFVI"), is the basis for an optimized NGCO platform. Aligning with the European Telecommunications Standards Institute (ETSI) specification and NFV architectural model, it adopts QCT NFV-designed platforms powered by the latest Intel technologies.

A number of key data plane performance related Enhanced Platform Awareness (EPA) features from Intel are implemented to boost VNF data plane performance. Each feature is adopted in OpenStack to enable optimal NGCO application deployment.

These technologies are briefly discussed in the following sections

Fast Data Path

In a typical cloud OpenStack environment, network traffic accessing the Internet passes through a virtual machine (VM), typically flowing through a complicated network virtualization stack that may include a test access port (TAP) device, Linux* bridge, virtual Ethernet (vEth) pair, and Open vSwitch* (OvS). To accelerate data plane packet processing, the NFVI supports memory huge pages in the compute nodes, through either OvS with the Data Plane Development Kit (OvS-DPDK) and/or single root input/output virtualization (SR-IOV), as shown in Figure 3.

Resource Allocation Strategy

Platform resource allocation and performance can be optimized through the use of two EPA-enabled features: CPU pinning and non-uniform memory access (NUMA) awareness. CPU pinning provides a one-to-one mapping between virtual CPUs (vCPUs) and physical CPUs, thus dedicating specific compute resources to individual VMs, as shown in Figure 4. This capability can increase cache efficiency and VM performance by preventing the virtual machine monitor (VMM) from continuously swapping out the contents of the cache (i.e., VM context switching). As VMs run on user-space tasks within the host operating system, CPU pinning provides similar advantages to task pinning.

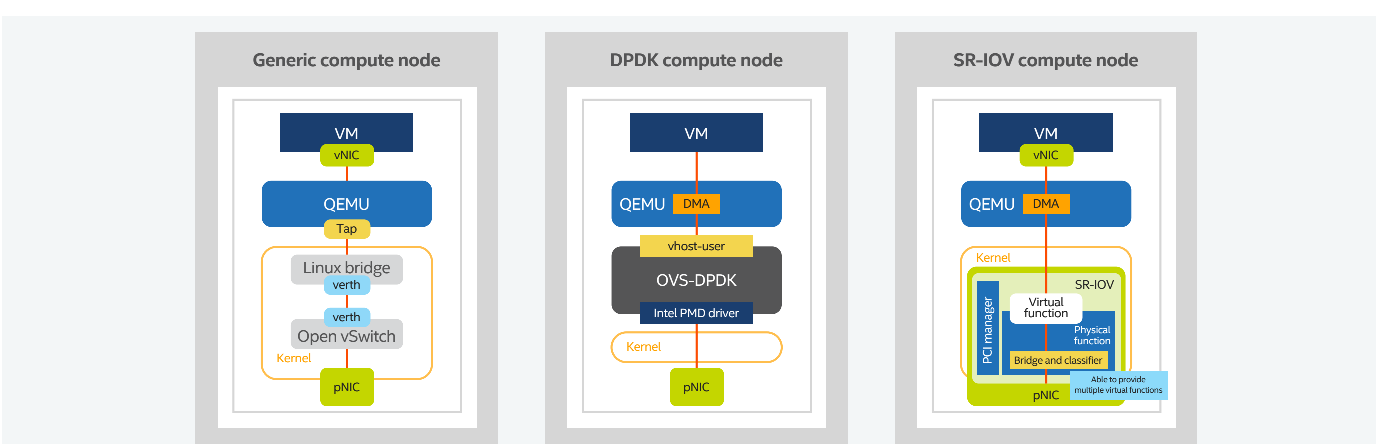


Figure 3. Data Plane Acceleration Techniques

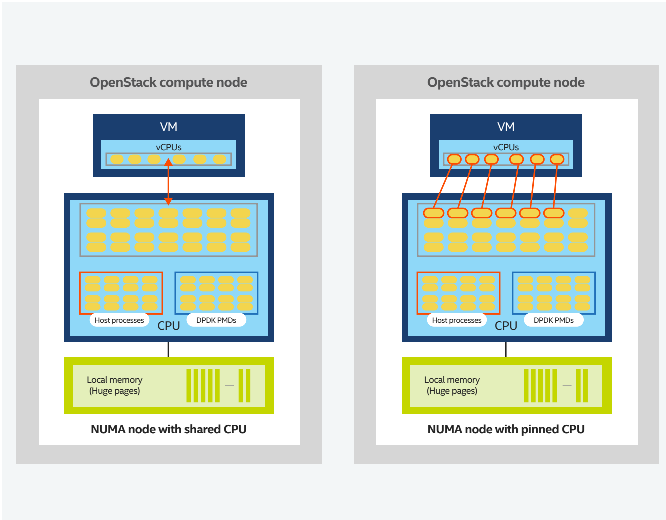


Figure 4. CPU Core Pinning

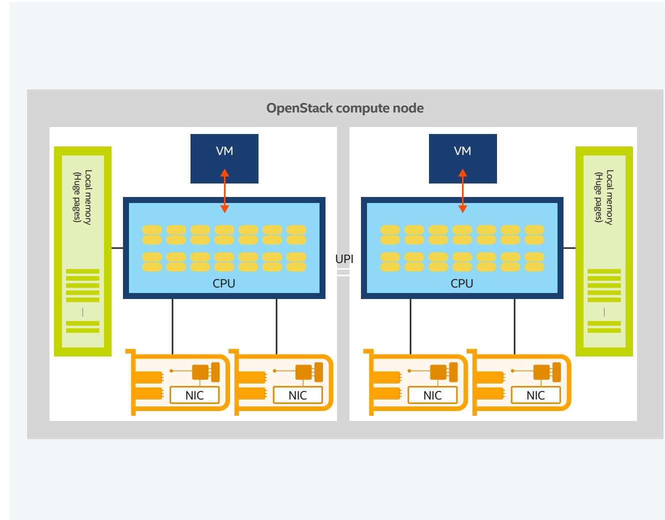


Figure 5. NUMA-Aware Architecture

NUMA-awareness is important in multi-CPU platforms because it ensures memory and I/O access are confined to a single CPU, resulting in higher VM performance. NUMA-aware architecture models can ensure VMs are assigned system memory that is physically connected to the CPU they are running on (i.e., Figure 5), which minimizes memory access latency and improves system determinism. For example, OpenStack Compute (nova), running on the OpenStack Platform, intelligently allocates memory when launching VM instances, which ensures optimal resources are assigned to performance-sensitive workloads , like NFV edge gateways.

The NFVI proposed in this paper takes advantage of a QCT NUMA-balanced design that supports local memory access and distributes NICs across CPUs and sockets in a NUMA aware manner.

Solution Functionality

NFVI can also be designed to fulfill the strict requirements of CoSPs and provide the following benefits:

- Flexible design with performance scalability
- Reliable design with high resource availability
- Efficient deployment using the auto-deployment tools

Network Functions Virtualization Workloads

To accelerate CoSP adoption of the NGCO, Intel and QCT have designed a blueprint for edge-Telco VNF workloads and collaborated with commercial independent software vendor (ISV) partners to deploy their VNF products onto an NGCO reference architecture. VNF services have been verified using an end-to-end validation process, which integrates the functions of user entity (UE), access network, core network, and applications. VNF performance was tested to ensure CoSP edge performance expectations are met.

The NGCO project sponsored by Intel and QCT incorporates components from an ecosystem of hardware and software vendors. The first stage will incorporate core and edge network functions, including a mobile Evolved Packet Core (EPC) from ASTRI* and a residential broadband network gateway (BNG) from netElastic*. The following sections describe the integration of the ASTRI EPC and netElastic BNG into the NGCO Rack.

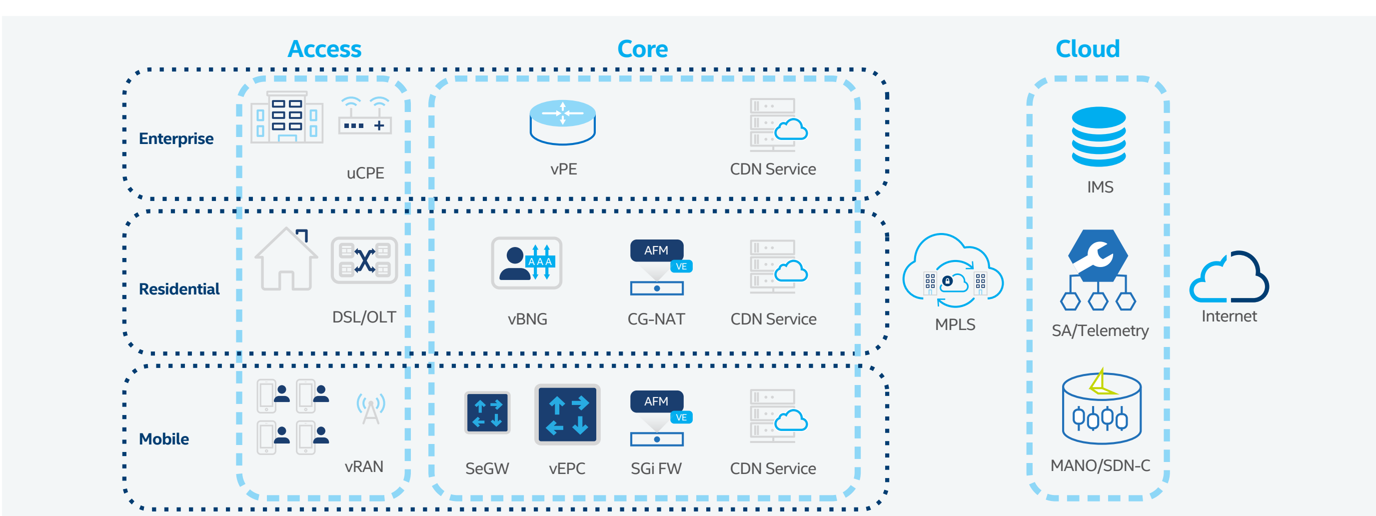


Figure 6. Next-Generation Central Office VNF Blueprint

Mobile Network Workload - ASTRI* Solutions

Although the 5G standards have not fully finalized , some mobile CoSPs plan to launch 5G trial service before the end of 2019. 5G technology will deliver more bandwidth, lower latency, and much greater connection capacity than its predecessors through the adoption of new specifications including enhanced mobile broadband (eMBB), ultra-reliable, low latency communications (URLLC), and massive machine type communications (mMTC). The 5G new radio (NR) radio access network (RAN) is expected to operate on the mmWave band (28GHz) for very high bandwidth applications, and the 5G core network will have greater capacity to process traffic. Adopting the NGCO approach, the appropriate service bandwidth can be expanded by adding data plane VMs as required.

The control and user plane separation (CUPS) architecture has been defined as the 3GPP standard for 5G core networks. ASTRI implemented the CUPS architecture in its next-generation mobile core (NGMC) software, which supports separate control plane and data plane VMs. The control plane VM provides MME, SGW-C, and PGW-C functions, and the data plane VM provides SGW-U and PGW-U functions. The data plane VM can be scaled-in or scaled-out based on the subscriber bandwidth requirements.

The ASTRI NGMC increases single node data plane performance by integrating the DPDK and dynamic device personalization (DDP) technology, which help accelerate data plane processing. The OpenStack passthrough feature is deployed on each data plane interface to further improve gateway user plane performance.

Intel tested the performance of the ASTRI NGMC running on a single QCT QuantaGrid* D52BQ-2U node configured with eight VMs: one control plane, six data plane, and one security gateway (SeGW), as shown in Figure 8.

The node NUMA balance design is based on the dual Intel® Xeon® Gold 6152 processors with six PCI-Express* (PCI-e) Gen3 x8 slots to CPU1 and two PCI-e Gen3 x8 slots with one Open Compute Project* (OCP) Mezzanine slot to CPU0.

Two PCI-e NICs are required for OpenStack infrastructure and the associated tenant network. To maximize performance across both CPUs, four data plane VMs are deployed on CPU1 and two data plane VMs on CPU0. The control plane VM uses the OpenStack tenant network to communicate with the data plane VMs and the S1-MME network. Each data plane VM requires Intel® Ethernet Converged Network Adapter XXV710 ports for data plane service, one for S1-U, and another for SGi, as shown in Figure 8.

Testing confirmed a single data plane VM can handle more than 40 Gbps of traffic with a packet size of 768 bytes. For the maximum performance configuration, the server can handle between 100 and 200 Gbps of traffic when using the

NFVI configuration shown in Figure 8.1

The security gateway (SeGW) VM provides the mobile security gateway function for encrypted communication between small cells, or the eNode B, and the core network signaling gateway. In order to increase crypto performance, the ASTRI SeGW should sit between the wireless access node and the EPC gateways and use the Intel® QuickAssist Adapter 8960 to accelerate IPsec encryption and decryption. The SeGW can handle more than 40 Gbps of encrypted/decrypted traffic with Intel® QuickAssist Technology (Intel® QAT) offloading enabled.

Fixed-Line Network Workload - netElastic* Solutions

The broadband network gateway (BNG) is the major network function of fixed-line networks for residential broadband subscriber service. From the user access side, traditional copper DSL access is being rapidly replaced by optical PON/OLT access to increase the bandwidth of work "the" last mile: between user residences and the central office. As the over-the-top (OTT) market (e.g., Netflix*, YouTube*, Apple* TV) grows, CoSPs face the challenges of supporting much higher network bandwidth and increasing the system capacity of residential networks. NFV solutions provide a demonstrated path to scalable, cost optimized solutions that will allow CoSPs to upgrade their networks.

Running on x86 commodity hardware, the virtual BNG (vBNG) offered by netElastic delivers more than 120 Gbps throughput on a single node. Its architecture, like the ASTRI NGMC, is based on the CUPS approach. The data plane can be extended to multiple data plane VMs with an SDN-enabled switch providing the traffic steering function.

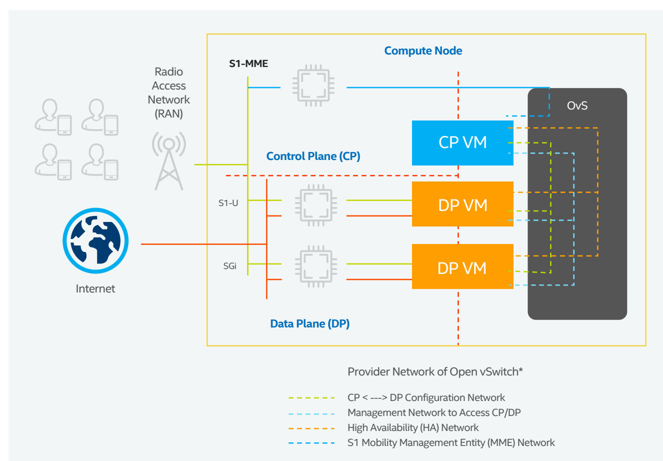


Figure 7. ASTRI* Next-Generation Mobile Core (NGMC) with Control and User Plane Separation (CUPS) Architecture

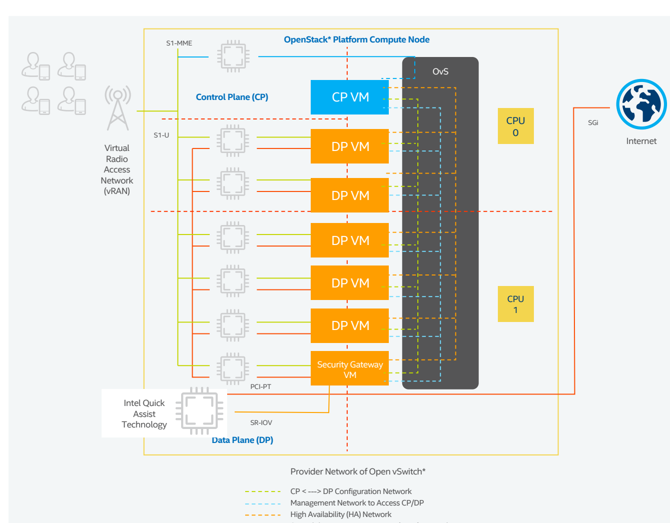


Figure 8. Instance Configuration

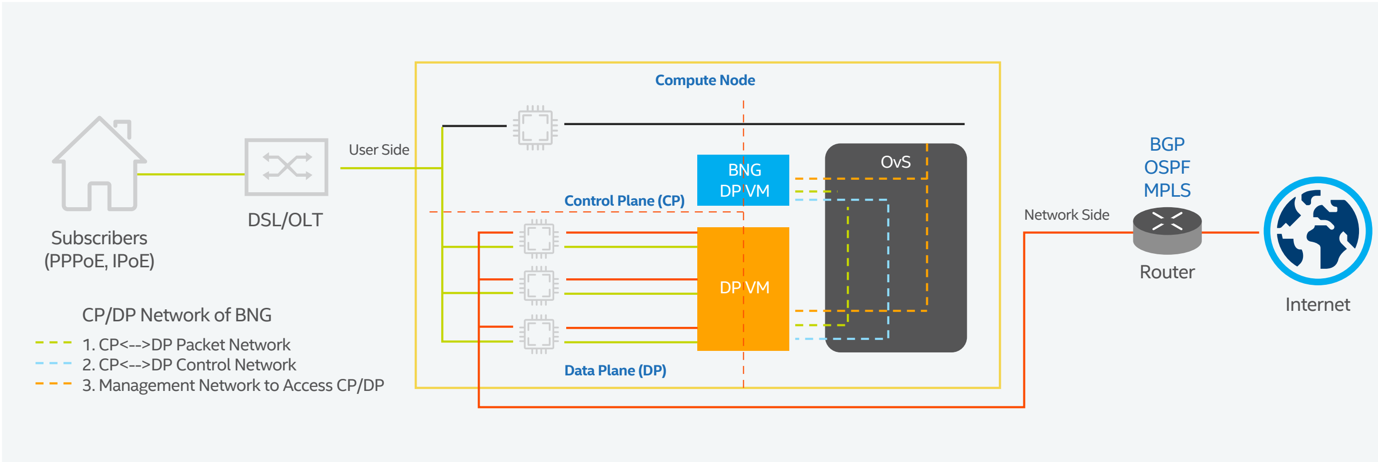


Figure 9. NetElastic Virtual Broadband Network Gateway (vBNG)

In general, the vBNG system will connect to an IP/MPLS backbone for Internet access. netElastic simplifies the network architecture by putting the virtual provider edge (vPE) router function into vBNG products, which handle IGP/BGP/MPLS routing protocol exchange with the IP/MPLS backbone network, as shown in Figure 9.

From the subscriber side, the user connects to the vBNG via the Point-to-Point Protocol over Ethernet (PPPoE) or Internet Protocol over Ethernet (IPoE) CPE client. From the network side, the backbone router exchanges routing information via the OSPF/BGP/MPLS protocols.

The vBNG control plane VM performs PPPoE/IPoE authentication in conjunction with an authentication, authorization, and accounting (AAA) server. The vBNG data plane VM processes the the PPPoE header (e.g. encapsulation and de-capsulation) and handles the routing and QoS policy for each subscriber.

The initial authentication packet is received by the data plane VM and is forwarded to the control plane VM where the authentication occurs. The control plane VM synchronizes the subscriber policy data (e.g., packet forwarding rules and policy) with the relevant data plane VM; thereafter, the user is authenticated and traffic flows through the system.

Like the ASTRI NGMC data plane VM, the netElastic BNG/PE VM is also deployed with PCI passthrough and utilizes DPDK technology to accelerate data forwarding.

The vBNG/vPE VM supported a throughput of 120 Gbps with 256 byte packets, measured using the Spirent* TestCenter*.2

Fixed-Mobile Convergence

A key trend in communications network architecture is to support the convergence of fixed-line and mobile workloads. This convergence is driven by the desire of Tier 1 CoSPs to provide both fixed-line and mobile network services to their subscribers through a bundled service offering. Subscribers can then seamlessly switch between mobile and fixed-line residential access based on location, fees, etc. To cost-effectively offer both types of network services, CoSPs can build a network infrastructure that can be shared by fixed-line and mobile services. Fixed-line/mobile convergence is one of the key concepts enabled by NGCO architectures. It allows fixed-line VNFs (e.g., vBNG) and mobile VNFs (e.g., vEPC) to be deployed on the same compute node infrastructure, as shown in Figure 10. Based on the VNF traffic profile models, operators can expand the capacity of BNG or EPC services on demand by adding more VMs, and by doing so, fixed-mobile convergence can be instantiated and adopted on the NGCO Rack.

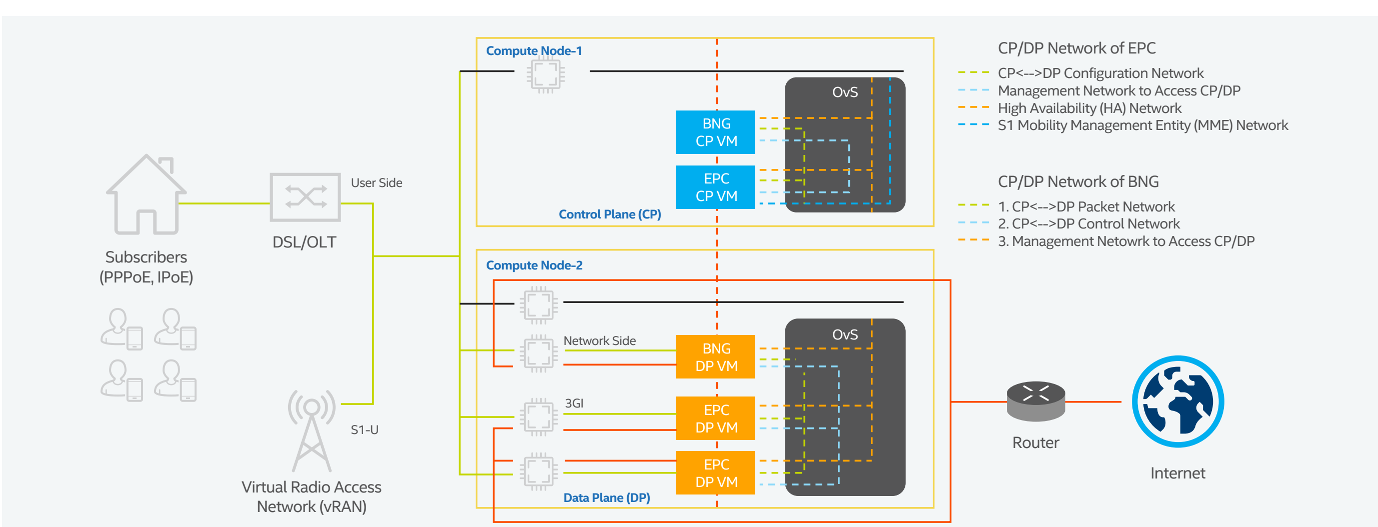


Figure 10. Enabling Fixed-Mobile Convergence

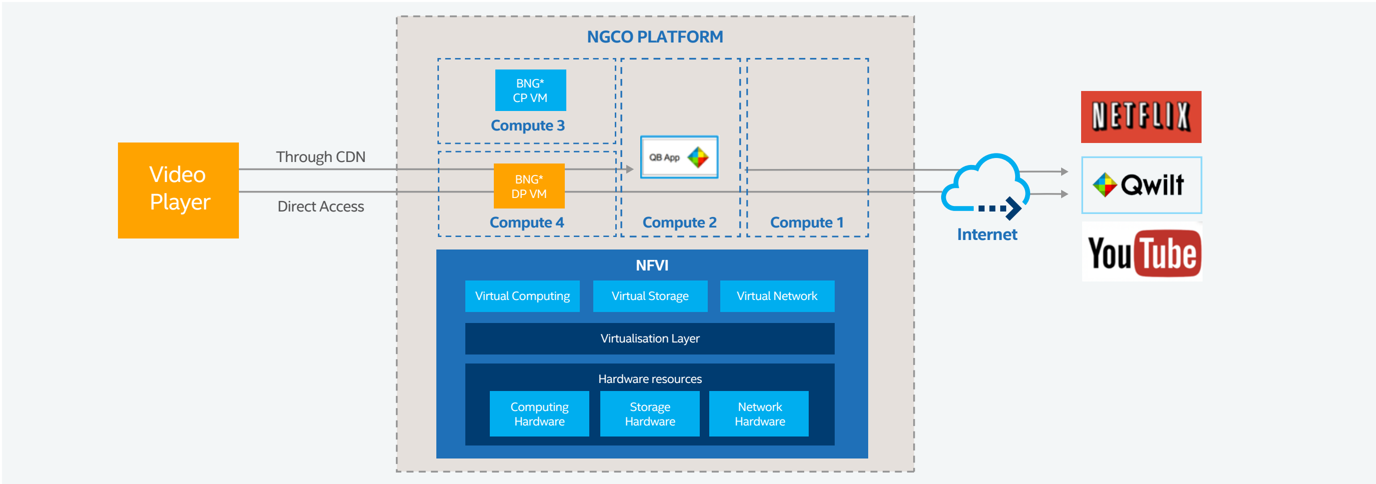


Figure 11. Content Delivery Network (CDN) Architecture

Security Workload – F5 Networks* Solutions

With an insecure Internet connected to the rest of the world, hackers can attack and steal important information and assets. In order to effectively protect CoSP Infrastructure from attacks and provide effective protection for users and application services, there is a clear need to integrate security protection into the NGCO Rack.

As a premier provider of data center technology, F5 Networks* offers security products, like the Advanced Firewall Manager* (AFM), which provide security protection to the CoSP edge data center. On the NGCO rack, F5 AFM is used to protect network service and subscribers. The firewall secures the SGi LTE interface, protecting application services, like CDN, video, and IP Multimedia Subsystem (IMS), and its carrier-grade NAT (CG-NAT) module hides subscribers' IP addresses and provides a level of protection against distributed denial-of-service (DDoS) attacks.

F5 AFM delivers packet processing capacity ranging from 500 Mbps to 40 Gbps with corresponding licenses. The F5 AFM VM supports PCI passthrough and SR-IOV to optimize performance, and any CoSP can deploy the AFM VM with multiple versions based on the bandwidth requirement of the protected target.

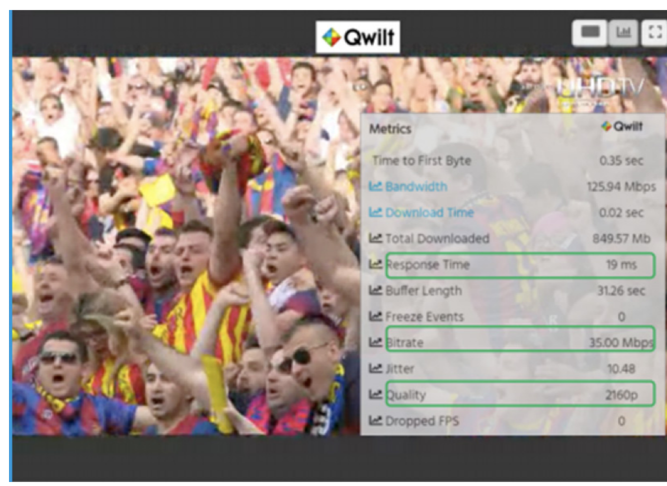
Application Services Workload – Qwilt* Solutions

A content delivery network (CDN) distributes content (e.g., HTML pages, javascript files, and videos) to the network edge and in close proximity of users, which reduces latency and increases availability, performance, and throughput. By minimizing the distance data travels over the Internet, CDNs deliver data more quickly to consumers at a lower transit cost. Telecom CDNs are deployed at the edge and in COs, regional data centers, and core data centers to form a distributed CDN infrastructure. The following discusses CDN service capability provided by Qwilt* in the NGCO.

Figure 11 shows how the Qwilt CDN connects through the BNG to enable an end-to-end, fixed-line network environment. In this example, the client has two video players: one connected directly to the origin server and the other connected to the Qwilt CDN with content caching. Both paths go through the BGN network.

The performance of both paths is shown in Figure 12. Since the Qwilt CDN caches the video, its path is higher performance than the direct path. The response time is more than nine times faster, the bit rate is more than four times faster, and the quality is two times greater.

Better response time
Higher bitrate
Streaming at 4k(2160p)



Slower response time
Lower bitrate
Streaming at 1080p

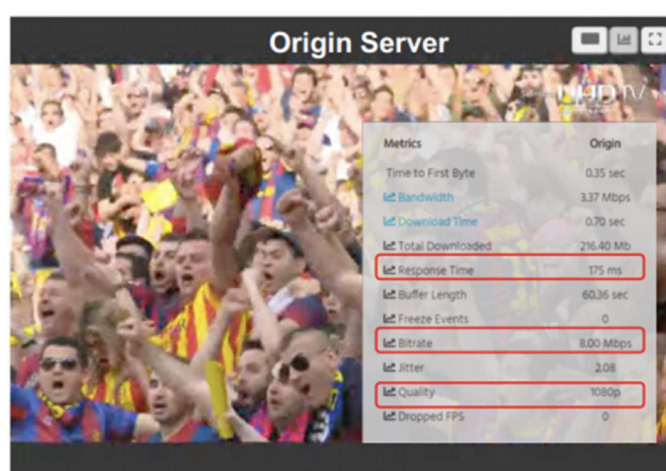


Figure 12. Performance Gain from Content Delivery Network (CDN) Services

Telemetry for Service Assurance

CoSPs implement network service assurance policies and processes to satisfy quality aspects (e.g., throughput and availability) as defined in customer service level agreements (SLAs).

With the rise of NFV, carriers around the globe are under pressure to provide competitive services to differentiate themselves from other CoSPs. Automating network functions, based on the reference architecture from telecom organizations like ETSI-NFV, is becoming critical to enable more agile operations needed to meet these business demands. To increase agility and service levels, CoSPs should consider digital transformation consisting of hardware infrastructure, upper layer NFVI, and VNFs, along with the management and orchestration (MANO) of services.

The QCT telemetry framework, shown in Figure 13, is a major part of the QCT service assurance solution used to automate the performance and visibility for OpenStack-based NFVI and VNF applications. This solution is designed to help CoSPs implement VNFs and services based on the ETSI-NFV reference architecture. In addition to VNFs and NFVI, QCT also integrates the physical infrastructure into a single pane of glass management system.

All Platform telemetry is made available from the platform collection agent, collected, using open industry standard interfaces and provided to orchestration and monitoring/ analytics systems.

Telemetry can be processed online and offline as required.

QCT integrates well-known, open-source software packages to build the foundation for its telemetry framework. For example, QCT uses collected which is an open source collection daemon which has been around for 10 years and used in many monitoring solutions. It has a very modular architecture which consists of mainly read plugins, which speak to various platform subsystems to retrieve stats or events, and also has write plugins or publishing plugins which are capable of publishing the telemetry to a number of interfaces.

Community plugins query the physical infrastructure to collect hardware telemetry, such as memory and storage size, CPU utilization, and peripheral matrix, using the Intelligent Platform Management Interface (IPMI). The NFVI virtual environment runs on QCT hardware, including a QCT-developed OpenStack plugin that retrieves data from OpenStack via the instantiated and adapted OpenStack API. There are two groups of VNFs running on the NFVI: the core VNF group and the application or service VNF group. EPC and BNG belong to the core VNF group, and the CDN and firewall belong to the application VNF group. Today, there is no common application/vendor specific NF telemetry interface; thus, QCT works with each VNF vendor to develop vendor-specific collectd plugins that are then adapted to the openStack API. The open-source libvirt plugin will be used in the future for Open Network Automation Platform (ONAP) integration and a VM monitoring mechanism.

Prometheus – a database of time-series metrics – is used to store the rich data sets from collected and provide data analytics processing. Prometheus not only stores metrics but also provides two features to enhance the QCT telemetry framework. The first feature is precision alerts, which are written in a flexible language and maintain dimensional information. Furthermore, the alert manager sends notification three ways: email, IM and pre-defined web-hook processes. With this feature, administrators receive timely notifications, allowing them to quickly address related issues. The second feature is a strong data query capability, supported by a flexible query language that allows slicing and dicing of time-series data used to generate ad-hoc graphs, tables, and alerts.

QCT telemetry framework supports six different dashboards (including the one shown in Figure 14) to provide the user with easy and clear information. Through these dashboards, administrators can fully comprehend the overall operation status visually on a single operations status pane.

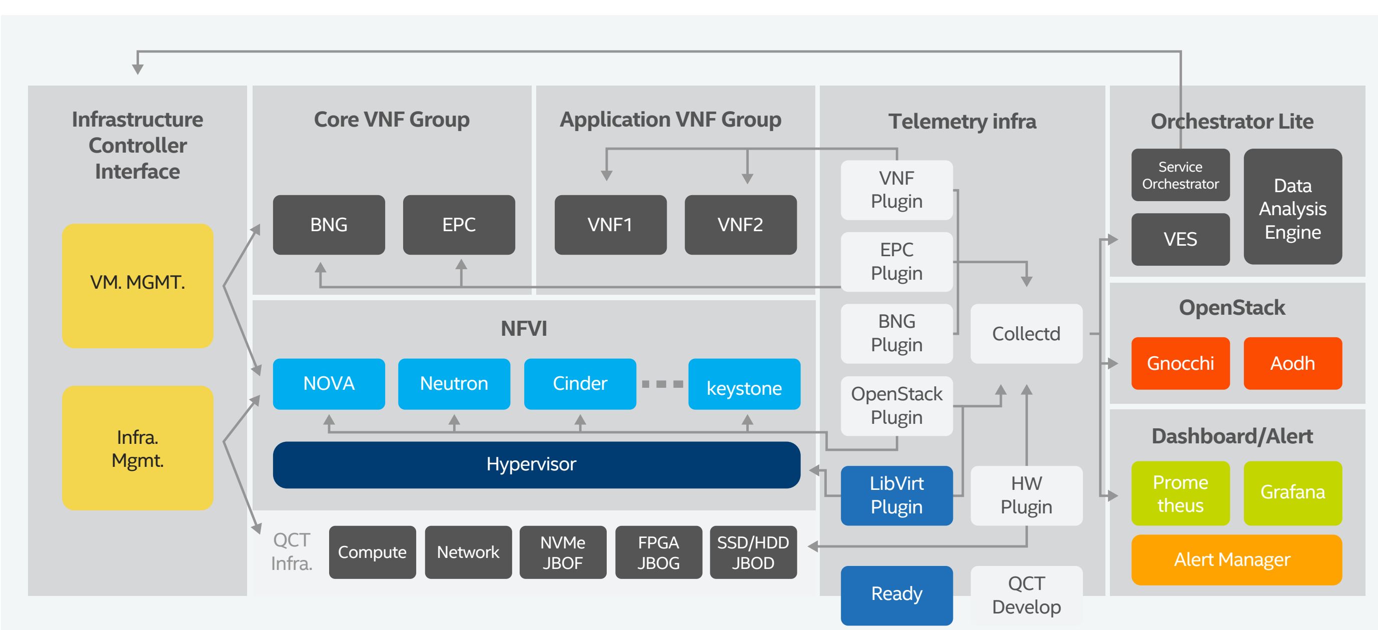


Figure 13. QCT* Telemetry Framework Architecture

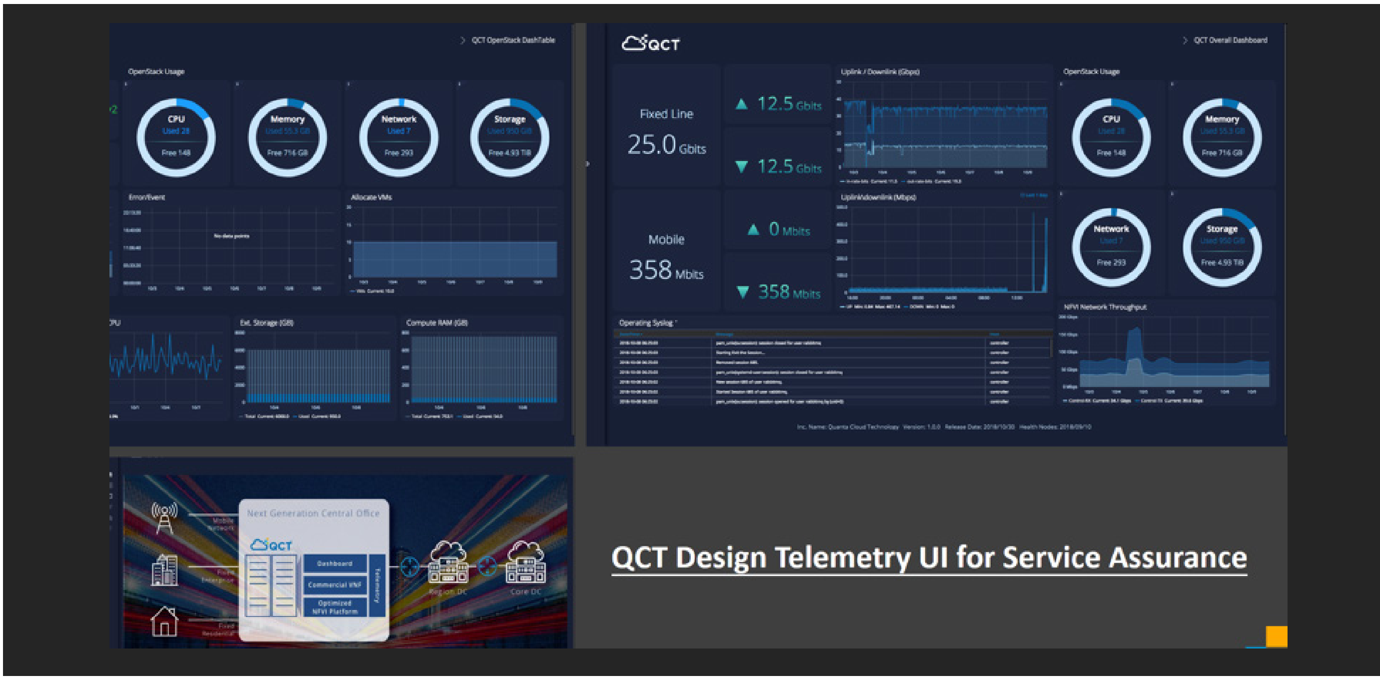


Figure 14. Telemetry Demo Dashboard

Next-Generation Central Office

The NGCO program integrates ONAP for its management and orchestration MANO solution. QCT designed a closed-loop automation use case based on the ASTRI EPC VNF. The scenario is shown in Figure 15

Several major ONAP modules are involved in this use case:

- The Data Collection, Analytics, and Events (DCAE) subsystem collects, ingests, transforms, and stores data, as necessary, for analysis. Furthermore, DCAE provides a framework for analytics development.
- Policy is a subsystem of ONAP; and it maintains, distributes, and operates on the set of rules that underlie ONAP control, orchestration, and management functions.
- Data Move as a Platform (DMaaP) is a premier platform for high performance and cost-effective data movement services that transport and process data from any source to any target with the format, quality, security, and concurrency required to serve business and customer needs.
- The Application Controller (APPC) is the generic application controller that receives commands from ONAP components, such as MSO, DCAE, or the portal, and uses these commands to manage the life cycle of services, resources (virtual applications and VNFs), and their components.

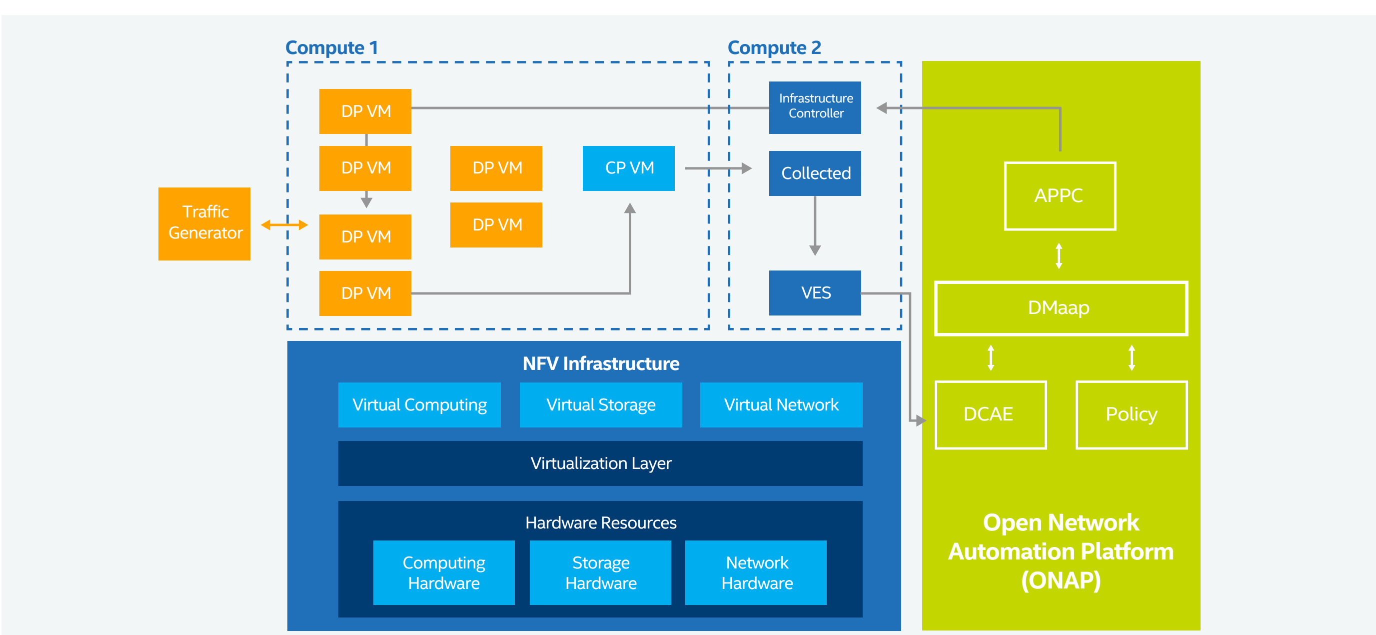


Figure 15. Closed-Loop Automation

The steps to demonstrate closed-loop automation are as follows:

- Initially, the ASTRI EPC runs with only one control plane VM instance and one data plane VM instance.
- The traffic generator is started. The data plane VM instance reports the subscriber number and current bandwidth to the control plane.
- Collectd sends metrics to the ONAP DCAE engine via the VES module.
- The traffic generator continues to simulate more subscribers and traffic.
- The DCAE subsystem senses when the subscriber number or bandwidth approaches the high critical threshold and informs the DMaaP.
- The Policy engine handles this event and sends the scale-out event to DMaaP.
- The APPC handles this scale-out event and sends a command to the infrastructure controller to initiate a scaling out operation.
- The infrastructure controller calls the OpenStack API to launch a new data plane VM instance.
- A new data plane VM registers to the control plane VM instance and requests to join the EPC service.
- The traffic generator continues to increase the subscriber number and the traffic level. The upward scaling operation continues until the number of data plane VMs reaches six.

Next-Generation Central Office Ecosystem

Service providers are adopting IT-based network approaches to reap the same flexibility, agility, and cost savings benefits as corporations. Increased agility can help CoSPs speed up the trial and launch of new applications to fulfill customers' expectations.

This proposed QCT NGCO solution establishes a VNF and location agnostic platform, which is possible because NFV decouples network functions from hardware and decouples network functions from locations. QCT provides edge products and solutions that enable CoSPs to deliver bandwidth-consuming and time-sensitive applications, such as CDN, augmented/virtual reality (AR/VR), and gaming, through a fixed or mobile virtual infrastructure.

As NGCO ramps, Intel and QCT will continue to work with different VNF partners to integrate, validate, and optimize their telecom workloads through seamless collaboration. The ever growing list of Tier 1 partners and their enthusiasm to participate in the NGCO ecosystem suggest great potential. QCT expects more solution partners to join the NGCO ecosystem and its network transformation journey.

Summary and Next Steps

NFV has become an extremely compelling choice for edge deployment, as it provides added flexibility and portability, enables greater economies of scale, innovative functions, and new business opportunities that were unthinkable through hardware-centric solutions.

NFV enables an alternative to traditional ASIC- and NPU-based networking platforms that deliver very high throughput but lack the flexibility and portability essential for agile edge deployments. These platforms are also expensive and very time consuming to develop, which are impediments to delivering new services.

Intel® architecture integrates a number of new technologies that further increase NFV throughput performance, reaching levels where industry-standard servers can comfortably support the deployment of network functions at the NGCO edge in a cost-effective way through a diverse ecosystem.

All this is delivered in a secure rack infrastructure that provides the requisite telemetry and platform analytics to enable management layers to address and correct issues in real time through emerging artificial-intelligence-enabled automation.

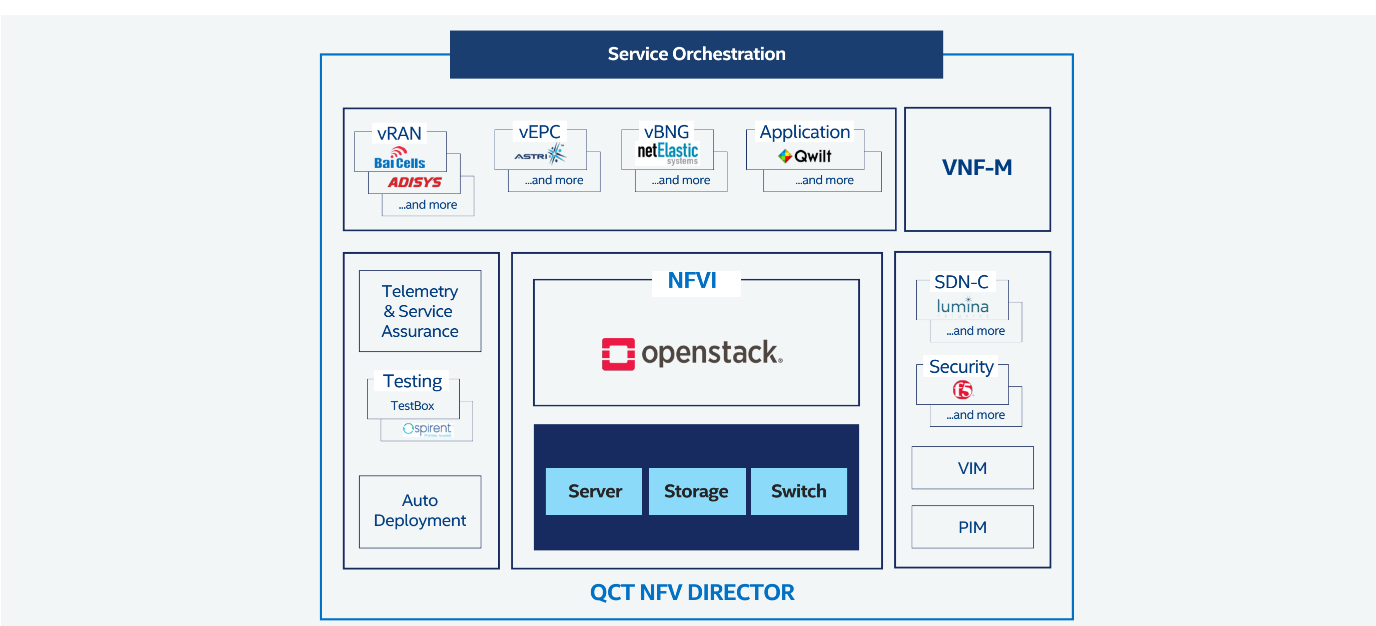


Figure 16. QCT* NFV Ecosystem

Quanta Cloud Technology (QCT) is a global datacenter solution provider, combining the efficiency of hyperscale hardware with infrastructure software from a diversity of industry leaders to solve next-generation data center design and operation challenges. QCT serves global cloud service providers and telecoms. Product lines include hyper-converged and software-defined datacenter solutions with a diverse ecosystem of hardware component and software partners. QCT designs, integrates and serves cutting edge offerings via its own global network. For more information, please visit QCT NGCO.

Links and References

For more information, please see "Creating the Next Generation Central Office with Intel® Architecture CPUs," which can be found at https://builders.intel.com/docs/networkbuilders/creating-the-next-generation-central-office-with-intel-architecture-cpus.pdf.

The 6153 NFV applicable Xeon SP SKU

https://www.intel.com.au/content/www/au/en/products/processors/xeon/scalable/gold-processors/gold-6152.html

Relevant information on the Intel Quick Assist Adaptor.

https://www.intel.com/content/www/us/en/ethernet-products/gigabit-server-adapters/quickassist-adapter-8960-8970-brief.html

Relevant information on Intel Dynamic Device Personalization technology.

https://software.intel.com/en-us/articles/dynamic-device-personalization-for-intel-ethernet-700-series

Relevant information on Intel's Service assurance the Telemetry technology

https://networkbuilders.intel.com/network-technologies/serviceassurance

http://f5.com/nfv

https://qwilt.com/5g-mec/qwilts-5g-mec-solution/

https://www.netelastic.com/index.php/products/vbng/

http://www.astri.org/

1. Source: Intel testing.

2. Source: Intel testing.

3. Source: Intel testing.

4. Source: Qwilt*

Acronyms	
AAA	Authentication, Authorization and Accounting Server
AFM	Advanced Firewall Manager (F5)
APPC	Application Controller
AR/VR	Augmented Reality / Virtual Reality
ASTRI	Applied Science and Technology Research Institute
BNG	Broadband Network Gateways
CoSP	Communications Service Provider
CDN	Content Distribution Network
CG-NAT	Carrier Grade Network Address Translation
CO	Central Office
CP	Control Plane
CPE	Customer Premise Equipment
CUPS	Control and User Plane Separation
DCAE	Data Collection, Analytics and Events
DDoS	Distributed Denial Of Service
DDP	Dynamic Device Personalization
DMaaP	Data Move as a Platform
DPDK	Date Plane Development Kit
DP	Data Plane
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ETSI	European Standards Institute
URLLC	Ultra Low Latency Communications
EPA	Enhanced Platform Awareness
FTTH	Fiber to the Home
FTTC	Fiber to the Curb
IMS	IP Multi Media System
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPoE	IP over Ethernet
ISV	Independent Software Vendor
LTE	Long Term Evolution
MANO	Management and Orchestration
MLPS	Multi Protocol Label Switching
MME	Mobility Management Engine
MMTC	Massive Machine Type Communications
NGCO	Next Generation Central Office
NGMC	Next Generation Mobile Core

Acronyms	
NFV	Network Function Virtualization
NFVI	Network Function Virtual Infrastructure
NiC	Network Interface Card
NPU	Network Processor Unit
NR	New Radio
NUMA	Non-uniform memory access
OCP	Open Compute Platform
OLT	Optical Line Terminator
ONAP	Open Networking Platform
OSP	Open Stack Package
OSPF	Open Shortest Path First
OTT	Over the Top
OVS	Open Virtual Switch
PCi-e	Peripheral Connect Interface Express
PE	Provider Edge
PGW	Packet Gateway
PON	Passive Optical Network
PPPoE	Point to Point Protocol over Ethernet
Intel QAT	Quick Assist Technology
RAN	Radio Access Network
SDN	Software Defined Networking
SecGW	Security Gateway
SGW	Signaling Gateway
SLA	Service Level Agreement
SR-IOV	Single Route I/O Virtualization
TAP	Test Access Point
UE	User Entity
VES	VNF Event Streamer
VMM	Virtual Machine Manager
VNF	Virtual Network Function