Huawei Technologies *Think Tech* >>>>>>>>>>>>>>>>

communicate

02/2017
ISSUE
82

Safe and secure in the clouds

Cloud Native goes beyond virtualization

Edge cloud goes 5G: MEC@CloudEdge

All Cloud starts at the core

Reconstruct to re-energize

Unleashing the power of networks

Scan for mobile reading

LET THE CLOUD HELP YOU RESPOND TO COMPETITIVE BUSINESS PRESSURES WITH EASE

Unleash the power of the Cloud and tap into the full potential of IT with Huawei's FusionSphere Cloud operating system

Huawei FusionSphere brings the future of Cloud computing technology here today. FusionSphere integrates with OpenStack architecture, aligns with developing industry standards, and fuses IT infrastructures with Cloud services to help you optimize IT resources, accelerate business, and capitalize on new opportunities!

For more information, please visit e.huawei.com

Innovative ICT Building a Better Connected World

Scan for solution details

HUAWEI

Sponsor:
Corporate Communications Dept.
Huawei Technologies Co., Ltd.

Editor-in-Chief:
Sally Gao (sally@huawei.com)

Editors:
Gary Marcus Maidment, Kyra Mi
Linda Xu, Julia Yao, Pan Tao
Xue Hua, Cao Zhihui

Art Editor:
Zhou Shumin

Contributors:
Li Chaoyang, Yuan Bo, Dai Libin
Liu Haofei, He Zhe, Liu Hao

E-mail: HWtech@huawei.com

Tel: +86 755 28786665, 28787643
Fax: +86 755 28788811
Address: B1, Huawei Industrial Base, Bantian, Longgang, Shenzhen 518129, China

Publication Registration No.:
Yue B No.10148

Sailing vertically into the new blue ocean

It’s been 156 years since James Watt invented the steam engine. Today, evidence of humanity's technological triumphs can be found in all corners of the world: from the tallest peaks to the deepest oceans, in the forms of roads, bridges, buildings, and other amazing physical legacies of human ingenuity.

Digitization is sweeping the globe at an increasing pace thanks to continual advances in IT, and every vertical industry is jumping aboard this new wave.

The communications industry has gone through three main phases of development. During its birth, the goal was to meet people's basic communications needs and expand the demographic dividend through access. Next, the Internet became pervasive thanks to communications networks, which quickly gave rise to the OTT applications that are flourishing across the planet today. In this second phase, the main goal was to expand the data dividend. In the future, IT will transform society and stimulate the digital transformation of all vertical industries. A huge market will be created and operators will play a crucial role as the cornerstone of global digital transformation.

There will of course be both challenges and opportunities. When moving into vertical markets, operators have to forge ecosystems and flexible business models that quickly respond to the market. But, their ability to do so is dependent on the strengths of their networks. After a century of existence, telecom networks face the momentous task of supporting transformation into a digital society. This will require reawakening their power with agile, intelligent infrastructure and operator platforms that position services like video, IoT, and cloud as new basic network services.

Huawei anticipated the trends of the information industry back in 2012 with its next-gen network strategy SoftCOM (Software-Defined Telecom Network). Based on All Cloud architecture and the latest SDN, NFV, and cloud tech, SoftCOM helps operators cloudify services, operations, networks, and hardware. It lets them centrally control and manage all network resources and pipe traffic to meet the fast-changing demands of upper-layer services.

Huawei is ready to help operators reinvigorate telecom networks, digitally transform industry, and explore the new blue ocean of verticals.

We believe that, "If you want to walk fast, walk alone; if you want to go far, walk together."

Zou Zhilei

Zou Zhilei, President of Carrier BG, Huawei

CONTENTS communicate ISSUE 82

Cover Story

Reconstruct to re-energize: Unleashing the power of networks

What are the 4 steps you need to take to make the move into cloud services and provide more than just connectivity?

P04

Experts' Forum

On top of the food chain: Creating value for operators with full cloudification

With data centers running the show, full cloudification is the way telcos can create true value

P10

Focus

Safe and secure in the clouds

The cloud creates a whole new network environment. But, it needs to be protected. Here's how to do it.

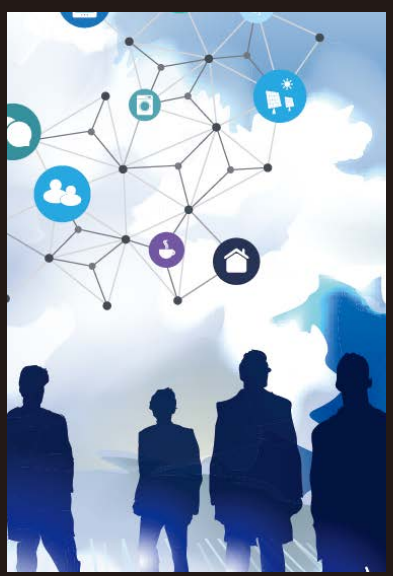
P14

Focus

Thinking outside the box with Integrated Telecom Cloud

Integrating IT and CT services and carrying them on the same platform was once impossible. Not anymore

P18



Focus

Getting down to business with CloudVPN

The B2B market is a new blue ocean. Telcos already have the right ships and fuel to set sail and look for this business treasure. Find the map here

P21

Reconstruct to re-energize

Unleashing the power of networks

Network transformation into a cloud-based business model lets operators provide more than just connectivity as simple network infrastructure service providers – it lets them make the move into the cloud service arena.

By Yuan Bo, Director of Network Architecture Transformation Dept., Huawei

Yuan Bo
Director of Network Architecture Transformation Dept., Huawei

Four main drivers

The decades and trillions of dollars poured into communications networks are proving to be no match for today's needs. Revenue and ARPU growth are slowing, efficiency is poor, TTM for new services is slow, and changes to user demands outpace operators' ability to meet them. OTT vendors are a new competitive force, and digital services are eroding revenues from voice and SMS.

There are four main drivers forcing operators to carry out ICT network transformation and combat these issues:

Services

Operators' main services in the future will include virtual, augmented, and mixed reality; cloud services; 5G and IoT; and HD video. Networks will need to carry these services and meet a slew of demands, for example, ultra-low latency, high bandwidth, high reliability, huge numbers of concurrent connections, seamless connectivity, security, rapid service provisioning, and quick and easy online customization.

User experience

Operators' digital services must deliver a ROADS experience: Real-time, On-demand, All-online, DIY, and Social. Traditional network architecture is unable to do so.

Operations and maintenance

Operators need intelligent and flexible future networks that automate distribution and deployment for agile O&M without the need for manual intervention. The real-time, automated adjustment of network resources would provide elastic scalability, automated fault isolation, and self-healing.

To compete with the service innovation capabilities of OTT players, operators hope to attract third-party (3P) partners – including OTTs – to deliver ROADS services to enterprises and users on next-gen platforms and digital markets. To make this possible, they need to integrate and open up network capabilities because 3Ps cannot easily develop services on traditional networks. But, reconfiguring network elements (NE) in a unified and dynamic way to expose network capabilities is far from easy.

TCO and total value of ownership (TVO)

Sluggish revenue growth for telcos is compounded by the need to invest increasing amounts into infrastructure due to the surge in data traffic, causing TCO to jump. The alternative – low resource utilization coupled with the increasing costs of capacity expansion – is unsustainable. Network transformation can cut TCO, boost TVO and resource utilization, and maximize ROI.

Network transformation can unleash the massive value of network infrastructure by creating an agile, open, and automated network that's cloudified and software-based with SDN and NFV. In a trend that will transform the telecom industry, networks will function as seamless service-enabling platforms on which telcos can provide IaaS, PaaS, and SaaS on a pay-per-use basis.

Unleashing the power

An immense undertaking, transformation involves services, architecture, networks, and operations.

Architecture

Operators need to cloudify their entire ICT network infrastructure with data centers (DC) at the

Transforming operations is more than just providing online customer services and online sales – it also needs to support process transformation with a focus on customer requirements

core. Information storage, processing, and exchange; service processing; and transactions will occur in DCs, which will also be the telephone exchanges of the future.

Future DCs will be distributed, and transformed from traditional DC infrastructure through cloud computing and SDN technologies based on the core concepts of physical distribution and logical integration.

Physical resources in the DC will be virtualized to form logical pools spanning multiple DCs. Virtual DCs (vDC) can then be provisioned from these logical resource pools for use by users or tenants, thereby linking multiple discrete, stratified, and heterogeneous distributed cloud DCs to form new distributed cloud DCs.

The distributed cloud DC model will support open and flexible architecture that enables integrated resource scheduling across multiple DCs through SDN cloud-and-network synergy. Resource utilization will be boosted, management simplified, and user experience improved. The cloud DC will not only carry telecom clouds, it will also support operators' private and public cloud services and provide integrated, unified ICT architecture.

Network transformation

Network transformation uses SDN and NFV to construct an agile, open, and automated operator network on top of cloud DC infrastructure.

SDN separates the forwarding and control planes, so entire networks can be centrally managed and controlled, vastly improving network resource allocation and efficiency. Using the SDN controller, northbound coordinator, and SDN applications, E2E services can be rapidly deployed and the following features can be automated: inter- and intra-DC networks, access networks, and WANs. SDN helps build a software-defined, programmable, application-oriented, and open intelligent network.

NFV is used to make NEs software based by decoupling software and hardware. Virtual network functions (VNF) run on a unified cloud DC-based NFV infrastructure (NFVI). NFV management systems and coordinators (MANO) allow the unified orchestration and lifecycle management of physical and virtual resources on the cloud architecture.

Combining SDN and NFV enables the network and NE functions to be software-based, accelerating new service development and deployment. It enables automated network deployment and elastic scaling based on current network traffic, and automates system management, including isolating faults and self-healing. SDN and NFV promotes new business models by utilizing network resources more efficiently, improving deployment and O&M efficiency, shortening service TTM, and opening up key network capabilities to third-party partners and developers.

Transforming operations

Transforming operations is more than just

providing online customer services and online sales – it also needs to support process transformation with a focus on customer requirements.

Digitization and Internetization will reshape operators' traditional business models. New, agile digitized operations, services, and O&M management on infrastructure will provide a ROADS service experience. A flexible XaaS model will meet fast-changing and personalized user requirements, and big data will play a key role in data-driven decision-making and intelligent operations.

Carriers' next-gen digitized operations systems will be more than just a platform or a software and hardware product, and will offer different capabilities to different users. For users, the next-gen operations system will be like an e-commerce platform where digital services and products, including operator or third-party products, can be purchased and customized.

Operators will be able to use next-gen operations systems to perform agile operations like developing new services and solutions and carrying out marketing campaigns. For commercial partners, it will act as a channel and service development platform that invokes network capabilities with open APIs. So, next-gen operating systems will in fact be a business enabling system for operators, partners, and end users.

Next-gen operations systems also need to support E2E service and resource orchestration and coordination across the entire network to enable the lifecycle, decision, and workflow management of network resources and automated O&M.

The next-gen operations system will be a business enabling system for operators, partners, and end users. It will also need to support end-to-end service and resource orchestration plus network-wide coordination.

Time to wake up

Network transformation is a long-term process that has three main objectives:

Awakening speed: accelerating new service TTM from several months to several days; improving response speed to user demand, with subscriptions and modifications completed online with immediate effect; and shortening service innovation cycles.

Awakening functions: increasing the performance of opening network functions, providing unified open APIs to third-parties, flexibly invoking third-party applications, monetizing network functions, increasing revenue, and innovating services.

Awakening efficiency: cutting TCO by optimizing network resource utilization and traffic scheduling, and reducing OPEX by centralizing and automating tool platforms and boosting network O&M efficiency.

To achieve these objectives, operators need to follow a stage-based strategic plan.

Four steps

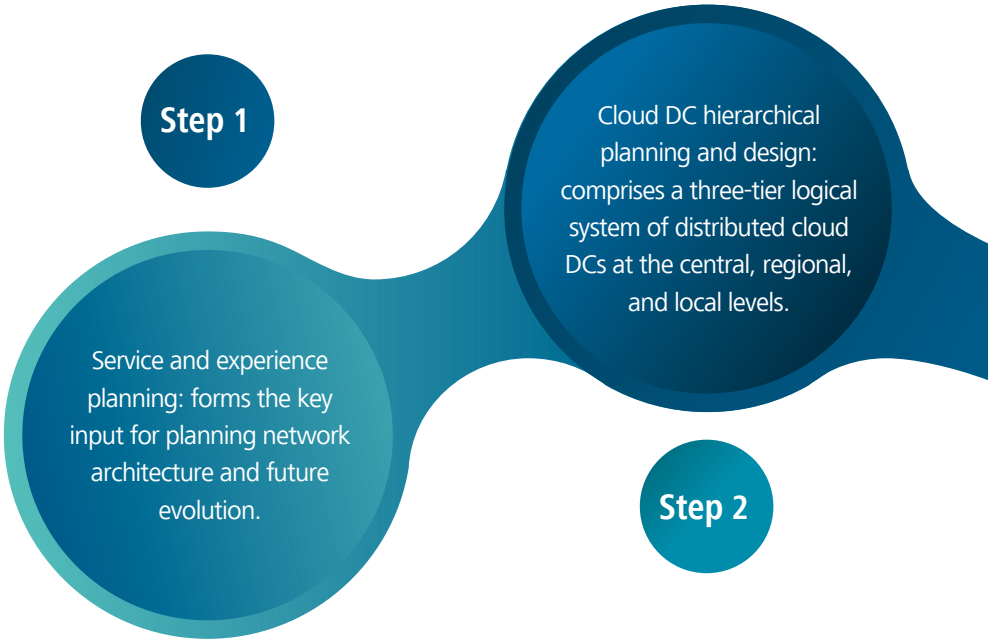
Step 1: Service and experience planning

Service planning involves generating roadmaps for operators' future services based on their business value, viability, alignment with strategic goals, and projected user numbers. Once the services are determined, experience planning can identify the main KQIs for user experience to incorporate into KPIs. These are used as key inputs for subsequent network architecture and evolution planning.

Step 2: Cloud DC hierarchical planning and design

Network architecture in the future will comprise a three-tier logical system of distributed cloud DCs at the central, regional, and local levels. Each DC tier will carry different services to meet different

SDN-based MAN and backbone networks will connect DCs to form agile end-to-end networks

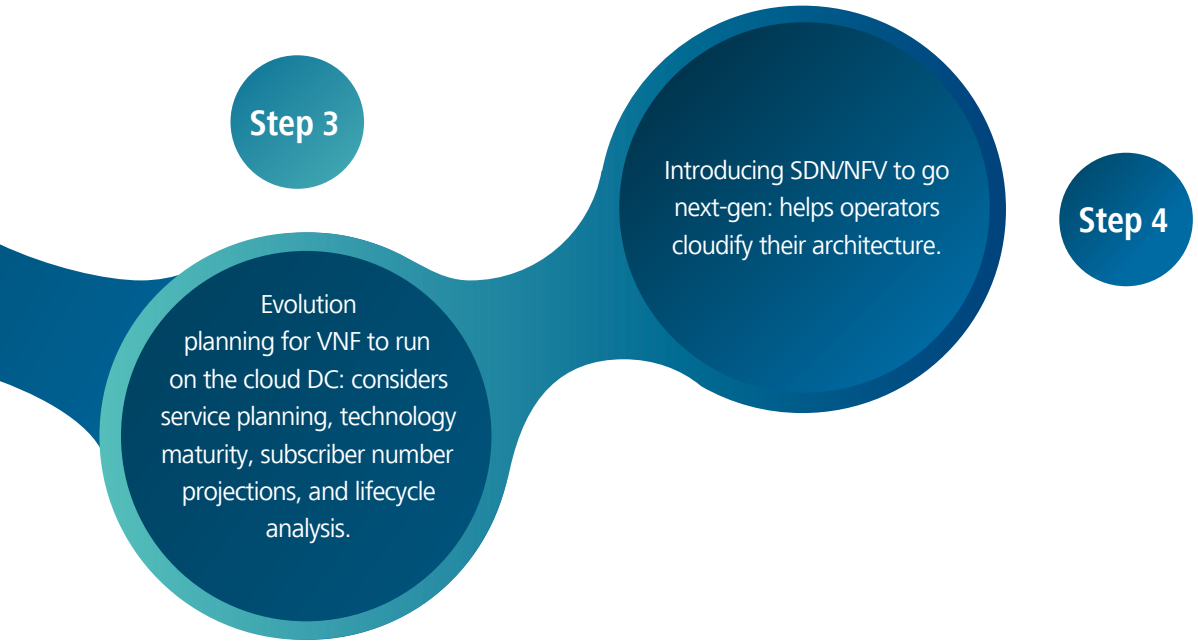


user experience demands. KPIs from early experience planning, such as latency and bandwidth, are crucial for selecting DC sites and designing hierarchy. Other factors that need to be considered include the deployment of existing network NEs, network topology and traffic, city and population, 2G/3G/4G coverage, and natural disaster distribution.

The central DC is usually used to carry centralized services such as public cloud services and centralized IT. The regional DC carries services with localized requirements or that contain sensitive information, for example, government and enterprise clouds, VAS, and provincial network or subsidiary network IT. Control plane and signal plane NEs can be centrally deployed in the regional DC. NEs where forwarding is sensitive because very low latency is required are mainly sent to the local DC. NEs on the user plane should be deployed down the network to the city-level, as close as possible to the end user to satisfy demands for services like HD video.

The three-tier division is just reference architecture that can be tailored to, for example, two or four tiers based on operator needs. For example, some NEs on the user plane where forwarding requires extremely low latency can be moved further down to edge DCs to meet the experience demands of future services.

SDN-based MAN and backbone networks will connect these DCs to



form agile end-to-end networks. Once planning is complete, designing and selecting the cloud DC infrastructure is necessary to deliver carrier-grade performance. This includes NFVI as well as utilities such as air conditioning, fire prevention, and power supply.

Step 3: Evolution planning of VNF run on the cloud DC

The evolution roadmap must take into account service planning, technology maturity, subscriber number projections, and lifecycle analysis on the existing network hardware. When VNF is implemented, current network equipment must be gradually replaced to ensure legacy network investment isn't wasted and services are smoothly migrated. SDN deployment takes the form of DCN > DCI > CloudVPN > SDN-WAN, and then develops from Overlay to Underlay. This centralizes and automates network control, creating a flexible, programmable network.

Step 4: Introducing SDN/NFV to go next-gen

When constructing a next-gen operating platform, the Infrastructure Enabling System (IES) orchestrates and coordinates services and resources E2E to support O&M management.

Step by step

Future transformation into cloudified network architecture takes time. Increasing network architecture elasticity and O&M agility and building capabilities must happen in increments.

In 2012, Huawei proposed the All Cloud architecture of the future: SoftCOM (Software-Defined Telecom Network). Open and unified, it can help operators cloudify hardware, networks, and services and internetize their operations.

Huawei has already completed many successful commercial trials of SDN and NFV with leading operators worldwide, with its OpenLabs in many countries involved in setting up open-source organizations and open ecosystems. Huawei hopes to build a new type of network for the future through collaboration and serve as the engine for network digitization.

On top of the food chain

Creating value for operators with full cloudification

Operators' digital business transformation starts with network reconstruction. As well as network cloudification, it requires upgrading equipment, networks, services, and operations, where all network functions and service applications run in data centers.

By Jiang Junmu, Chief Correspondent, C114

The Cloud 2.0 era has arrived. Over the next 10 years, an estimated 85 percent of enterprise applications will migrate to the cloud. Some operators are responding to market forces as their walled gardens are being smashed down, while others are actively embracing the future, speeding up evolution towards integrated intelligent information services providers.

Network reconstruction with data centers at the core is a prerequisite for successful digital transformation. Providing digital services and innovating business models depends on flexible architecture, agile network O&M, and having the right organizations and capabilities to support them. Pipes that can meet consumer demand for a ROADS experience and move with the cloud are a core capability that operators need to be competitive in vertical industries and restructure the value chain.

Jiang Junmu
Chief Correspondent, C114

However, network cloud evolution is a lengthy process and virtualization is just the start. Transformation involves both IT and CT as it will require constructing open-source IT systems, maintaining carrier-grade reliability, and protecting operators' existing investments. New, challenging issues are emerging such as long integration times for multiple vendors and complex cross-layer fault location.

The entire industry will need to come together to explore how operators can re-activate network infrastructure to unleash the true power of the pipe.

Beginning with the trends

Many leading operators have set transformation plans in motion, including AT&T (Domain 2.0), Telefonica (UNICA), Deutsche Telekom (PAN-EU), China Mobile (Big Connectivity Strategy), and China Telecom (Transformation 3.0). All the major technology providers are developing technology plans and customized solutions for digital transformation.

The transformation trend has arisen from real-world pressures faced by operators and customers' changing requirements. With integration between the digital domain and the real world accelerating, the communications market is currently in a stage of growing pains.

Challenges threatening the industry include dwindling demographic dividends, the decreasing prominence of traditional services, and declining traffic revenues. For example, figures from the Ministry of Industry and Information show that people in China sent one-third less text messages during the 2016 Spring Festival compared with 2015, but mobile users consumed 2.6 times more Internet data.

Society is undergoing a process of informatization. Services and applications that were originally defined in terms of computers and network ecosystems are now described in terms of user experience. Consumption methods and behaviors are changing profoundly, with a growing reliance on the Internet.

Huawei embodies customers' demands as ROADS: Real-time, On-demand, All Online, DIY, and Social. To meet ROADS requirements, operators need greater capabilities for agile operations; they need to build open, collaborative ecosystems to open network capabilities, accelerate service TTM, lower OPEX, and innovate digital services.

Traffic trends

Thanks to video and cloud computing, operators have a chance to return to the top of the value chain. Video now accounts for over 50 percent of network traffic, which will grow to 80 percent over the next three to five years. If operators don't embrace this change, video will become a huge burden. But if they do, the opportunity exists to turn it into a new basic service.

Then there's the vertical industry sector, which is set to grow into a new blue-ocean market worth trillions. A new industrial revolution is upon us, as evidenced by initiatives like Industry 4.0 and Made in China 2025. This evolution will be defined by how industries adopt Internet models to upgrade, rather than by the penetration of the Internet into industry. By 2025, the market value of digital transformation in vertical industries will reach an estimated US$150 million. The application of video in vertical industries will also grow rapidly, promising to be part of daily experience.

When it comes to verticals, operators have many natural competitive

Huawei's All Cloud strategy proposes that operators upgrade their equipment, networks, services, and operations models, and cloudify their networks

advantages like branding, nationwide network infrastructures, data centers in the areas they serve, and a wealth of government and enterprise customers. Moreover, numerous operators, such as Deutsche Telekom, BT, and Orange, run their own separate enterprise businesses.

Statistics show that the Internet-based enterprise service market in China has skyrocketed since 2015. While investors, innovators, and tech giants are already competing in this highly competitive market, operators will still have an opportunity to provide enterprise customers with a number of carrier-grade B2B services such as cloud data centers; public, private, and hybrid clouds; cloud leased lines; and cloud security. Deutsche Telekom, for example, recently joined forces with Huawei to launch Open Telekom Cloud, a public cloud IaaS offering.

Network 2020

Operators' traditional siloed network architecture doesn't enable the service innovation and growth required in the cloud and video age. By 2019, for example, predictions hold that traffic will total a massive 10.4 ZB. Equally, network traffic models are also changing because content is now centralized in data centers, while new applications like IoT require more diverse network service capabilities.

The user- and application-centric networks that will mature by 2020 will help safeguard the position of operators as digital enablers. Huawei's All Cloud strategy proposes that operators upgrade their equipment, networks, services, and operations models, and cloudify their networks. They can then create hardware resource pools, achieve fully distributed software architecture, and automate their systems. Data centers will form the core of the network and run all network functions and service applications. SDN and NFV will drive transformation into Network 2020 architecture. SDN will open network capabilities, providing flexible and dynamic support for service requirements. NFV will integrate basic service infrastructure and allow physical resources to be flexibly allocated. Transforming the network into a software-defined, cloudified network using SDN/NFV will create an efficient enabling platform for services.

AT&T developed an extensive network reconstruction plan called Domain 2.0 as early as 2013. The operator's aim was to transform its traditional hardware-centric network architecture into an SDN/NFV-based virtualized network. As part of the plan, the operator hopes to virtualize 75 percent of its network by 2020.

In 2013, Vodafone announced its Everything Moves on Cloud strategy, embodying its vision to migrate everything to the cloud, including network functions, consumer and vertical industry applications, and internal IT systems. The operator aims to reduce costs, enable agile operations, cut service TTM, and compete in more markets. In July 2015, with Huawei's full support and assistance, Vodafone Italy announced the launch of the world's first cloud-based commercial VoLTE network.

The three major Chinese carriers also view SDN/NFV-based network architecture transformation as the key to digital transformation. China Mobile announced NovoNet 2020, an ambitious vision for combining SDN and NFV technology, to build a next-gen network that features global resource scheduling, fully open functionality, scalable capacity, and flexible architecture.

China Unicom released its CUBE-Net2 white paper, outlining its vision for future network evolution. The strategy proposes using SDN, NFV, and cloud tech to reconfigure its network to cut OPEX and boost service capabilities. Similarly, China Telecom's Transformation 3.0 strategy will integrate network and IT integration resources on a simplified, integrated, agile, and open network using SDN, NFV, and cloud tech.

Virtualization is just the start

Operators are already using NFV to standardize and virtualize ICT network hardware. However, virtualization is just the beginning, as cloud evolution won't happen overnight. It's a long-term, phase-based process involving open-source IT systems coupled with CT reliability.

Cloudifying network layers will run from control to forwarding, core to edges, and from new to existing infrastructure. Huawei divides operator network cloud transformation into three main stages: Virtualization, Cloudification, and Cloud Native.

Virtualization is characterized by software and hardware decoupling in which IT and generalized hardware increase resource utilization and reduce costs network-wide. However, as virtualization only allows basic hardware and software decoupling, E2E elasticity and flexibility isn't possible.

Virtualization alone doesn't fully utilize cloud tech in communication networks, so operators must consider reconfiguring and decoupling their entire software systems and enhancing automation and scheduling coordination. Doing so will maximize the flexibility and elasticity of the entire network and improve system resource utilization and performance.

In 2015, operators and technology providers started to further decouple software systems into more granular software services like load balancing, stateless service logic processing, and distributed databases. These smaller discrete software services are scheduled flexibly and deployed separately, improving resource utilization network-wide.

The **cloud native** stage will begin in 2017 at the earliest. Based on cloudified networks, cloud native will feature disruptive technologies such as network slicing, agile infrastructure, micro services, and containers. Cloud native will feature a new ICT operating model that will enable agile business and create mutual success for operators, third-party developers, and end-users.

Getting down to business

Digital transformation is a high-risk, uncertain, and very expensive long-term endeavor, and not something that operators should undertake alone.

Huawei's SoftCOM and All Cloud strategies set the direction for network architecture transformation, and Huawei has already partnered with 60 operators worldwide in over 30 SDN and 130 NFV commercial projects.

Its CloudVPN solution helps operators develop enterprise digital services in three major service scenarios: cloud data center, cloud leased line, and cloud VAS. With the help of leading technology providers like Huawei, operators can achieve cloud native, cross-domain capabilities and reap the commercial rewards of both their legacy investment and digital transformation.

Safe and secure in the clouds

Transforming network security is intrinsic to network transformation. NFV and SDN are the tools for ensuring that operators can meet business requirements with a security system that adapts to the new environment network-wide.

By Lu Kunlun

New demands

Service-driven, cloud-based network transformation brings a slew of financial and performance benefits to operators, including greater service agility, faster service provisioning and TTM, lower OPEX, automation, the Pay-as-you-Grow model, and VAS.

But, traditional security mechanisms are no longer up to the task of protecting cloud environments for a number of reasons:

Ineffective static security software and hardware: The traditional static security components and software deployed on the network borders and servers cannot sense east-to-west traffic between virtual machines (VM) or ensure security in cloud scenarios.

Complex security management: Large cloud data centers (DC) have numerous cloud security policies, placing high demands on personnel to manually handle application, review, and configuration tasks such as policy updates, approvals, and around-the-clock maintenance.

Access and backbone transmission networks are still largely based on traditional architecture. As a result, NFV and SDN security features are applied mainly in the core network and cloud DC applications.

Diverse security needs

New network architecture creates different security requirements in different locations, as demonstrated in the following four scenarios.

One: vEPC requires signal security, so the security infrastructure must provide functions such as 3GPP IPSec encryption.

Two: The security requirements of vMSE include high-performance NAT and URL filtering, as well as Anti-DDoS.

Three: Security requirements for vCPE include border protection for enterprises with end-to-end VPN encryption, E2E QoS, IPS, and anti-virus.

Four: The IT Cloud provides telecom VAS like video for operators, which needs tenant-grade perimeter security.

The virtualized and cloudified infrastructure in each of these scenarios requires NFV-based security services. Scenarios three (vCPE) and four (IT Cloud) involve enterprise border protection and tenant protection, respectively. So, they require network equipment scheduling, including hardware boxes and vSwitch virtualized components, meaning that security must be integrated into the SDN network and adapted to the entire network architecture.

NFV-based security

NFV-based security involves processes for achieving the following three goals: software-based security infrastructure, micro security services, and high-capacity clusters with elastic scalability in cloud architecture.

Software-based security infrastructure applies to different sizes of software and hardware security components. Next-Generation Firewall (NGFW) hardware is deployed at every perimeter on the cloud DC network in the traditional manner, while the software version of NGFW is deployed on every VM. When VMs are launched, the software firewall or security service agent must also be launched.

Hardware and software NGFW must support 1:N and N:1 virtualization. 1:N virtualizes a single NGFW software or hardware device into many virtual devices that can be invoked by different servers or services based on NFV service requirements. N:1 pools multiple NGFW software and hardware components, so security resources can be flexibly invoked based on service needs. In both scenarios, the flexibility and ease of use of the software and hardware NGFW makes managing 1:N and N:1 virtualization easier.

Micro security services applies scheduling on individual and combined services. Virtual NGFW (vNGFW) includes more than ten types of security services, including application identification, NAT, VPN, IPS, and URL filtering. For easy deployment, these services can be batch deployed on a single vNGFW. For greater flexibility, distributed deployment can run each virtual security NE (or VM) as a virtual network function, with the Service Chain invoking the corresponding security service when they're used.

In SDN networks, security devices must support an open northbound interface

High-capacity clusters and elastic scalability implements high-capacity clusters to better support high-volume operator pipe services, with two possible implementation methods. The first is distributed architecture, where different modules of a vNGFW, such as URL filtering, VPN, and IPS, are deployed on different VMs. The multiple VMs are arranged on a single vNGFW to form a high-capacity cluster. The second method deploys each vNGFW on a single VM, and a cluster is formed by bundling multiple VMs. Once the vNGFW has formed a high-capacity cluster, security gateways of various sizes can be formed according to service requirements. This ensures the security of different traffic volumes and services within the cloud DC.

Security for SDN

In SDN networks, security devices must support an open northbound interface. The SDN controller can then carry out scheduling, micro-segmentation and, preferably, different controller ecosystems so they're effective in multi-vendor hybrid networks.

Heading north

Integrating security into an SDN network depends on security NEs that can be automatically deployed by the controller platform, so that services can be provisioned based on the Service Chain. Scheduling threat protection on-demand can provide minute-level service provisioning through Plug & Play; customized services such as automatic provisioning, expansion, and recovery; and the flexible directing of traffic flow.

The service process of the security NE is as follows: The external user or VM sends a first packet stream. After the stream passes the vSwitch, the vPath carries out policy-based packet analysis. After the vSwitch identifies a new stream, the designated virtual FW (vFW) inspects the stream, which is then sent to the corresponding vFW. The vFW implements the ACL policy and caches the ACL policy to the vSwitch. If the policy allows, the packet is sent to the target VM. Otherwise, it's discarded.

When the security NE is scheduled by the controller, it needs to collaborate closely with the vSwitch and other cloud network components. Thus, it assumes true responsibility for security in the virtualized network.

Micro-segmentation

Traditional DCs use perimeter security technology, including NGFW and IPS components. They carry out immersive analysis on inflowing traffic to confirm threats, and apply security policies like blocking and passing to allow authorized users or service flows to access DC resources. Typically, these security devices can only analyze north-to-south traffic, that is, traffic that enters and exits the DC.

However, east-to-west traffic now comprises the dominant volume of traffic in a cloud DC. The traditional method of defining security zones based on IP no longer meets the security requirements of cloud DCs for two reasons: one, cloud DC NEs have evolved from traditional single component hardware to VMs; and, two, users accessing the cloud

DC have evolved from traditional fixed network users into dynamic tenants and mobile and IoT users.

Micro-segmentation tech has changed the traditional method of defining security zones by IP. Security groups can now be defined on more parameters, for example, OS, device name, security tag, VLAN and MAC address. This particularly suits the dynamic security groups of cloud DCs such as dynamic virtual NEs, dynamic tenants, and dynamic remote access users.

Security NEs in cloud DCs must be able to support micro-segmentation, identify the security group of any traffic based on parameter and label, report to the controller, and accept and execute the security policy issued by the controller.

The controller ecosystem

When building cloud DCs, different operators use different controllers and network equipment from multiple vendors depending on specific requirements and existing infrastructure. Having this choice is an important way operators can reduce CAPEX and OPEX. As a result, it has become essential for security devices – as components of the SDN network in the cloud DC – to support management and orchestration via multiple types of cloud platforms and controllers, as well as multiple hypervisors. This capability determines whether security components can be widely adopted in cloud DC networks.

In a cloud DC, three methods of security management exist: the cloud platform (including third-party cloud platforms), the controller, and the traditional network management system. Security NEs support management by the cloud platform.

For open-source cloud platforms, security NE management plug-ins must be released to the open-source community for certification. For third-party cloud platforms, security NEs must be adapted to the third-party vendor. For the security NE to support SDN controller management, the northbound interface – normally RESTful – needs to be open and able to interoperate with the corresponding vendor's controller. The northbound SNMP and CLI interfaces of the security NE must remain open, as there will still be a need for independent network management systems for a long time to come.

In cloud DCs, the hypervisor and vSwitch direct and schedule virtualized traffic, as east-to-west traffic between VMs does not pass any physical firewalls. As a result, security vendors' virtual firewalls are often unable to function independently. Security NEs must therefore adapt to the main hypervisor and vSwitch. If they don't, security management and control won't be effective.

Operators are future-proofing their networks through cloudification, and adapting security to this new cloud architecture is an essential part of the process. Huawei's NFV-based security infrastructure fully supports SDN networks, enabling operators to simplify O&M, reduce TTM, enable flexible scheduling, and utilize resources efficiently to achieve business success as well as robust network security.

Thinking outside the box with Integrated Telecom Cloud

Today's trend for ICT transformation driven by data centers involves network-wide evolution. By constructing new data centers and transforming existing ones, Huawei's Integrated Telecom Cloud integrates IT and CT services and carries them on the same platform. Operators can rapidly deploy and provision services, elastically scale capacity, and integrate clouds for NE services, NFV clouds, and private clouds.

By Hu Jie

How operators see it

After passing the incubation and POC stages, SDN and NFV – two of the most popular transformation technologies – are being commercialized. Operators are transforming their NE service silos into virtualized, cloudified architecture, and deploying shared platforms with multiple Virtualized Network Function (VNF) services. This helps them decouple software and hardware, accelerate service innovation TTM, raise efficiency, and cut OPEX. A major IT strategy for siloed architecture has been to cloudify support applications, like BSS, OSS, big data, and OA, on private clouds.

Previously, it was assumed that true joint management and resource sharing between CT and IT services was impossible. Now, though, the integration of private and telecoms clouds into one cloud on a shared infrastructure layer is something that's increasingly viable.

Benefits

- Raises efficiency by connecting departments on a shared service platform for maintaining IT and CT applications.
- Eliminates information silos and integrates scattered resources, improving resource utilization.
- Integrates and decentralizes management and monitoring through a One Cloud Two Domains system for private and NFV cloud services.

Challenges

- Simultaneously meeting the differing system requirements of IT and CT services that coexist on the same platform.
- Ensuring simple O&M and adapting to the changes in organizational structure.

Integrated Telecom Cloud

As an infrastructure solution for telecom cloud, standard NFV Infrastructure (NFVI) is fully open and offers carrier-grade performance and reliability.

By transforming existing data centers and constructing new ones, IT and CT services can coexist. The Integrated Telecom Cloud solution allows telecom and private clouds to share IaaS and carry IT and CT services at the same time, meeting the diverse requirements of different services under unified management. The cloud also supports multiple data center SDNs, which is implemented on top of standard NFVI.

Shared platform

CT services and IT services have different requirements; for example, some CT data plane services demand high throughput and separately configured accelerator boards. The Integrated Telecom Cloud allows CT and IT services to share a single cloud running on multiple distributed data centers. The services also share virtual resource pools like KVM, VMware, and XEN; physical resource pools; and container technology.

Integrated Telecom Cloud enables cloud-network synergy and carrier-grade performance for carrier-grade latency and throughput, and prioritizes hardware acceleration for telecom cloud services, unified management, and O&M monitoring.

More importantly, it's based on open-source OpenStack architecture, which decouples layers and supports heterogeneous third-party software and hardware systems.

Automated data center networks

E2E network automation, SDN-based internal data center network automation, and network collaboration in and between data centers are all made possible with IT and CT services on the same cloud. Streamlining Layer-2 networks between data centers also enables automated resource

deployment and flexible capacity expansion.

Unified service orchestration and management

An integrated coordination layer is required to plan and coordinate services and carry out rights-based management and monitoring on all physical resources, virtual resources, and upper-layer services.

Taking the pain away

The Integrated Telecom Cloud removes information silos by forming single clouds from distributed data centers, and allowing these clouds to share resource pools. The single cloud improves user experience, speeds up TTM, and improves resource utilization. Moreover, resources can be elastically scaled, while E2E unified management solves issues with heterogeneous resources, multi-vendor equipment, and complex O&M.

Operators' legacy investments are protected by decoupling software and hardware, which in turn enables open ecosystems.

The bottom line

Compared with standard NFVI, Huawei's Integrated Telecom Cloud delivers major commercial value in three main areas:

On-demand resource allocation: The hierarchical decoupling of software and hardware transforms hardware into a resource pool where network function NEs are based on distributed data centers. Resource allocation is then on-demand.

One-click configuration of network functions: The resources and configurations required by network functions, such as computing, networks, storage, and security services, are configured on an integrated platform.

Dynamic adjustment of network functions: Software-based functions enable instant adjustments to be made on application operations like installation, deletion, migration, and capacity expansion and reduction.

Integrated Telecom Cloud handles design and automates O&M for all back-end COTS hardware and software. Its full range of services includes NFV application migration, application loading, cloud resources, and standardized applications for native cloud.

Operators can focus on front-end services, service innovation, and business development rather than worrying about the platform, giving a true out-of-the-box user experience.

The solution in action

Huawei's Integrated Telecom Cloud helps operators evolve single services into multiple services, single data centers into multiple data centers, and NFV to SDNFV (converged SDN and NFV).

As part of América Móvil's Network 2020 strategic plan, Huawei is integrating 41 of the operator's data centers across 19 countries into four logical data centers over the next five years. Features include an integrated operations framework that will transform a high quantity of existing siloed applications into an integrated resource pool for unified cross-data center service management.

So far, Huawei's Integrated Telecom Cloud has helped the customer slash service TTM from six to nine months to one week and cut TCO by 25 percent. The solution's open NFVI platform already smoothly runs Huawei, Cisco, Affirm and other third-party NFV.

As a cornerstone of an integrated ICT cloud, the Huawei Integrated Telecom Cloud can help operators transform into a future where IT and CT act in concert.

Getting down to business with CloudVPN

Huawei's CloudVPN solution helps operators enter the B2B enterprise service market by playing to their inherent advantages. Compared with OTT players, operators can offer stricter SLA guarantees, more secure connections, flexible bandwidth customization, and a broader range of services.

By Wang Yinghui, Xiao Baoquan & Chen Yuansi

B2B: A trillion-dollar market

With the B2C market beleaguered by sluggish growth and increasing competition, the B2B market is something of a treasure trove, with rapid growth currently seen in leased line services and cloud data center (DC) services. Alongside big data and IoT, operators will soon have the opportunity to provide enterprise customers with carrier-grade B2B services such as cloud DCs; public, private, and hybrid clouds; cloud leased lines; and cloud security.

Operators worldwide are thus beginning to shift their focus, with AT&T's Domain 2.0 strategy, Vodafone's Ocean strategy, Deutsche Telekom's OTC public cloud, and Telefonica's UNICA project all targeting the B2B space.

Market research by Analysys Mason shows how operators' overall revenues will decline slightly over the next five years, but the percentage of B2B revenues will rise as the B2B market develops into a trillion-dollar industry from now until 2020.

Operators' service system silos and closed networks are the main obstacles to developing B2B services. On traditional networks, new service provisioning from application to launch can take up to three months, upgrading and maintaining CPE equipment is inordinately expensive, O&M is inefficient, and innovation is inhibited. Moreover, intense competition from OTT players increases the risk of serious user churn and places operators on the competitive backfoot.

Operators need to develop new business models, formulate innovative services, and transform their network architecture. To achieve these aims, SDN and NFV are vital technologies.

Cloudy with SDN/NFV

Huawei developed its CloudVPN solutions

Fully cloudified B2B services cannot be implemented overnight, because business models, service processes, and network architecture are all involved

specifically to help operators provide enterprises with virtualized and fully cloudified B2B services on SDN/NFV networks.

Comprising CloudDC (data center), CloudVPN (leased lines), and CloudVAS/CloudEC (enterprise cloud communications), CloudVPN allows operators to out-compete OTT players with stricter SLAs, secure connections, and flexible bandwidth customization.

Solution breakdown

CloudVPN is an integrated service platform that offers carrier-grade cloud DC, cloud access, and VAS in an open ecosystem. It has four main components:

CloudDC: virtualizes resources and dynamically orchestrates services, which pools the resources of multiple DCs, automates service provisioning, and provides visualized O&M.

CloudVPN: applies Overlay technology for rapid connectivity, on-demand bandwidth adjustment, self-help services, and tenant-based performance monitoring and optimization. Diverse access methods are provided at the enterprise side, including low-cost thin CPE and x86 platform-based thick CPE with virtualized network functionality.

CloudVAS/CloudEC: CloudVAS includes security and WAN acceleration. CloudEC offers CloudPBX, CloudVC, and CloudUC. The solution leverages Virtual Network Functions (VNF) and flexible service chain functionality to provide diverse network VAS, including firewall VNF (with security functions such as anti-DDoS, DPI, IDS, and service awareness), load balancing VNF, WAN acceleration, and integrated enterprise communications. Enterprise customers can remotely upgrade and manage internal enterprise communications via portals. Coordinating enterprise cloud communications and the SDN controller enables dynamic QoS, location tracking diagnostics, and intelligent routing, allowing for visualized service operations.

CloudWAN: includes SDN evolution solutions for existing networks; SDN-based MAN, transmission networks, and backbone networks, with VNFs including vPE/VRR/vOTN; and newly built WAN networks such as OpenFlow MAN switches.

3 deployment phases

Fully cloudified B2B services cannot be implemented overnight, because business models, service processes, and network architecture are all involved. Deploying CloudVPN is dependent on E2E network evolution, including the DC, enterprise access, and the MAN.

CloudVPN deployment should be divided into the following three phases:

One: deploy cloud DC services so the enterprise can migrate applications to the DC provided by the operator. CloudDC enables resource pooling from multiple DCs, automatic service provision, and visualized O&M. Cloudifying enterprise leased lines and

traditional CPE services optimizes connectivity. The CloudVPN/ CloudCPE sub-solutions realize online subscriptions and the rapid launch of leased line services, plug-and-play CPE, dynamic bandwidth adjustment, and visualized traffic monitoring and optimization.

Two: deploy cloudified VAS on top of cloudified leased line services, providing operators with new sources of business growth such as cloud security, CloudEC, and MAN acceleration services. CloudVAS/EC sub-solutions enable flexible, on-demand, and PAYU provisioning of enterprise VAS.

Three: virtualize and fully cloudify network functions on top of cloudified services. This enables seamless connectivity between enterprise and cloud by using Underlay and Overlay networks for elastic bandwidth, and optimizes network performance based on service awareness. Network slicing fulfills a diverse range of on-demand commercial requirements such as vertical industry requirements, 5G backhaul, 4K video, and IoT.

Less worry, less effort, less cost

Compared to traditional B2B services, SDN/NFV-based CloudVPN services can help operators tap into the blue ocean market of enterprise services by bringing new commercial value, including flexibility, on-demand provision, high efficiency, and manageability.

On-demand: CloudVPN can help operators to provide network services on-demand, thus enabling enterprise customers to subscribe to network services based on their service needs in real time or in advance. Minute-level, automated service provision is possible for services like on-demand bandwidth adjustment, rental servers, CPU and databases, launching cloud security services, cloud-end multimedia communications, and audio and video conferencing. This enables network service and network resource flexibility and on-demand applications, meeting the growing and ever-changing service requirements of enterprises.

Experience: CloudVPN helps enhance user experience, allowing enterprises to subscribe to services and remotely upgrade VAS on a self-help portal. Customers can also monitor network usage in real time; for example, when two users use a voice service, the cloud communications server sends the call and quality data to the SDN Controller, which then uses the automated network policy and QoS configuration to optimize the call.

Efficiency: CloudVPN can manage network services more efficiently. CloudVPN services provide management via the operator, allowing remote O&M, which cuts costs. Visualized monitoring on cloud communications quality allows network traffic loads to be monitored and paths optimized automatically in real time.

CloudVPN helps enterprises reduce investment in equipment, because they can lease different kinds of network services from operators on a monthly or on-demand basis. Enterprises can focus on developing their core businesses by handing network services over to the operator, who can then provide one-stop services and management. For the enterprise, this means less worry, less effort, and less cost.

With SDN and NFV, CloudVPN achieves next-gen cloudified network architecture, helping operators bring innovative new business models with diverse, new, and reliable network services to the B2B market. This will increase customer loyalty, attract more SME customers, and emphasize operators' competitive advantages over OTT players.

The unique advantages CloudVPN offers maximize the commercial value of SDN and NFV and lay a strong foundation for operators to access and benefit from the lucrative B2B market.

Cloud Native goes beyond virtualization

Cloudification is more than just about resources: it's the comprehensive transformation of architecture. There are three phases involved: Virtualization, Cloudification, and Cloud Native. Cloudification and Cloud Native are both methods for achieving full network cloudification.

By Liu Hao, Senior Marketing Manager, Cloud Core Network, Huawei

The way to All Cloud

In October 2012, 13 leading operators jointly established the NFV-ISG group at the European Telecommunications Standards Institute (ETSI) to push NFV forward. The objectives of NFV-ISG cover decoupling the software and hardware in traditional telecoms equipment; implementing telecoms network functions on general-purpose computing, storage, and networking devices; enhancing management and maintenance efficiency; and strengthening system flexibility.

After more than four years of development, NFV technology is relatively mature and developing rapidly. Standards organizations, open-source communities, operators, and equipment vendors are working together to push forward the development of the NFV industry chain.

According to *Heavy Reading*'s June

Huawei "All Cloud" Strategy

2016 survey, 96 percent of telcos have started network cloudification. The survey also showed that 45 percent plan to complete full network cloudification before 2020. AT&T, Vodafone, Telefónica, Deutsche Telekom, China Mobile, China Unicom, China Telecom, Etisalat, and Ooredoo have all released network transformation strategies and objectives for 2020.

Huawei's All Cloud strategy aims to build efficient and agile telecoms networks that can help operators succeed by satisfying user demand.

The core of All Cloud strategy upgrades the network, equipment, services, and operations. All Cloud enables hardware resource pooling, fully distributed software architecture, and fully automated operations. It maximizes resource sharing; provides high scalability, elasticity, and reliability; and fully automates deploying services, scheduling resources, and handling faults.

Three phases to full cloudification

Cloudification is more than resource virtualization – it involves comprehensive architectural changes that enhance efficiency in R&D, service provisioning, and operations.

The full cloudification of carrier networks (All Cloud) takes place over three phases: Virtualization, Cloudification, and Cloud Native. Cloudification and Cloud Native are both methods for achieving full network cloudification. Huawei adopts the design concepts of cloudification from the outset to provide higher flexibility and reliability.

Virtualization

In this phase, software and hardware decoupling allows multiple network functions to be deployed on unified generalized hardware. This improves resource utilization. However, virtualization alone cannot achieve the full elasticity and flexibility of the entire system. The majority of solutions on the market today are still aimed at the virtualization stage, and are far from being true cloudification solutions.

Cloudification

Virtualized software architecture is optimized and reconstructed through cloudification. Network functions are cloudified, enabling fast delivery, smart O&M, and service innovation. System flexibility and elasticity are maximized, and resource utilization and performance further improved.

Cloud architecture: The new system must support three-layer software architecture comprising distributed load balancing, distributed databases, and stateless service processing units. It can complete elastic scaling in seconds without interrupting ongoing sessions, improving resource utilization and service elasticity and ensuring that carrier-grade capabilities are independent from hardware infrastructure. The new architecture also introduces automated service and resource orchestration, improving the flexibility and elasticity of the entire system.

Rapid delivery: Cloudified architecture needs to be completely open and support different kinds of generalized hardware and cloudified operating systems. Equipment from multiple vendors can be integrated with completely open cloudified architecture. The risks with multi-vendor integration are drastically reduced by performing integration testing on NFV network architecture in multi-vendor environments, verifying software and hardware solutions, and pre-integration. This shortens deployment time, allowing for fast delivery.

Smart O&M: Technological innovations, such as KPI-based health checks, self-healing, and multi-DC-based disaster recovery, can achieve five nines carrier-class reliability on cloudified networks. Smart tools, including performance evaluation and E2E

The concept of Cloud Native amalgamates different ideas, including DevOps, continuous delivery, micro-services, agile infrastructure, Conway's Law, and organizational restructuring based on commercial capability

fault demarcation/location tools, enable fully automated service deployment, on-demand resource orchestration, and rapid fault recovery and self-healing. These technologies and tools allow for agile and smart O&M on cloudified networks.

Service innovation: Using cloudified architecture, carriers can provide a one-stop network capability exposure platform for third-party partners. The platform can provide an integrated operations model covering the entire service lifecycle, including development, testing, deployment, and O&M. On the platform, telecoms resources – such as voice, video, location, QoS, and third-party applications – are packaged into APIs or SDKs, and shared with partners. This accelerates new service innovation and deployment, benefiting both operators and partners.

Cloud Native

The concept of Cloud Native amalgamates different ideas, including DevOps, continuous delivery, micro-services, agile infrastructure, Conway's Law, and organizational restructuring based on commercial capability.

Cloud Native integrates cloud computing technologies and enterprise management methods, enabling companies to migrate services to cloud platforms more efficiently and quickly. In doing so, they can gain the high efficiency and on-demand resource allocation capabilities of an All Cloud system.

Cloud Native has three major business drivers: elasticity, robustness, and agility. It introduces key architectural support technologies that expand and enhance the original components of the cloud system. Cloud Native is a natural evolution of the cloud system.

Elasticity: Network-level distributed architecture is the core. The key technologies are control and user plane separation, unified service chain, control plane reconstruction, and cross-DC deployment. These enable on-demand deployment based on service awareness, meeting the experience requirements of different applications.

Robustness: Network-level and service-level smart O&M capabilities are the core. The key technologies are network-level redundancy, active fault detection and self-healing, and big data service management. These enable high reliability, independent of infrastructure.

Agility: Network slicing, programmability, and grey release are the core. The key technologies are microservices, data model driving, and application orchestration. They enable the rapid and flexible release and deployment of new services for an optimal balance between resources and performance.

When operators evolve to the final Cloud Native stage, network functions can be flexibly assembled, network services can be released at any time, and network O&M and service operations will be fully automated. As a result, carriers gain unparalleled flexibility, efficiency, speed, and

elasticity. They are able to rapidly deploy services and their operating efficiency is greatly enhanced. They can quickly meet the needs of different network application scenarios and differentiated business demands. And they can agilely and flexibly meet the service requirements of vertical industries. At this point, carriers have achieved a true All Cloud network.

Of course, the commercial application of Cloud Native is not an easy or quick task. Various challenges exist that need to be overcome, including microservice decomposition, telecom-level service management frameworks, resource orchestration management frameworks, and limitations in container technology. And application depends on the actual circumstances of the services themselves.

For operators, the path to All Cloud is a long and complicated evolution process that involves the complete transformation of all aspects of the telco's business, including network architecture, organizational structure and personnel, and procurement, business, and operating models. It also requires open collaboration across the entire industry chain, including operators, infrastructure providers, software providers, and service providers.

Huawei provides full support to help carriers achieve All Cloud, which can be replicated by the entire industry.

Success stories

Vodafone is one of the industry's most forward-looking telcos. With its "Everything moves on Cloud" vision, the leading carrier has embraced next-gen network architecture and technologies. Vodafone's vision is to migrate everything onto cloud, including networking functions, consumer and vertical industry applications, and internal IT systems. It aims to reduce costs, accelerate new service TTM, and enable agile operations. In July 2015, Vodafone Italy collaborated with Huawei to launch the world's first cloud-based commercial VoLTE network, marking a milestone that year.

Huawei has established NFV Open Labs in China's Xi'an, in Silicon Valley in California, and in Munich, Germany. Bringing together operators, partners, and industry organizations, the labs combine verification and joint innovation to accelerate the commercialization of NFV solutions.

In Q2 2016, Huawei and a number of operators formed strategic partnerships, since which time more than 90 commercial cloud networks have been or are currently being deployed.

Huawei and Telenet deployed Europe's first commercial VoWi-Fi network in Belgium, and Huawei also rolled out the first Evolved Packet Core (EPC) network in Europe with Monaco Telecom. In the UK, Huawei and Hutchison deployed the world's first cloud-based Diameter Routing Agent (DRA) network. In another first, Huawei and Ooredoo deployed the first commercial cloudified network in the Middle East. Ooredoo and Huawei jointly picked up the Infrastructure Innovation Award at the Global Telecoms Business (GTB) Innovation Awards 2016 for this project.

Huawei was awarded Best Cloud/ Virtualized IMS Solution Award at IMS World Forum 2015 for the second time, following its first win the previous year. In 2016, Huawei was awarded the prize for Innovation in PCRF (Policy and Charging Rule Function) virtualization at Policy Control Conference 2016 and Best Network Virtualization Product at LTE Latin America.

Building more open, innovative, and healthy industry ecosystems deepens collaboration. Together, Huawei and its partners will create more innovative services and commercial value for carrier customers to drive the full cloudification of operator networks.

CloudVPN: Service deployment has never been faster or easier

CloudVPN is Huawei's new generation enterprise VPN solution. It greatly simplifies service deployment for operators and provides convenient and flexible service options for enterprise customers, including on-demand enterprise interconnection services and VAS.

By Xu Rui

Hello, Cloud

Enterprises are migrating their services to cloud, gradually replacing services that use Internet broadband access with VPN interconnections, security, and voice services. However, three main problems exist with traditional enterprise VPN solutions:

One: A long provisioning period. Enterprise customers cannot obtain services quickly, because operators need an average of 30 working days to provision VPN services.

Two: Enterprise VPNs are expensive to provision and maintain. Enterprises have to pay a lot for bandwidth, service hardware, and maintenance engineers.

Three: Operators only provide VPN connectivity, and more complex services require on-site deployment and maintenance. In addition to connecting company branches, enterprises need to deploy other functions, such as security, voice, load balancing, and WoC, to support cloud service deployment. This is a major undertaking.

A VPN solution supported by SDN and NFV technologies can resolve all these issues. The innovative service model of Huawei's new CloudVPN solution supports plug-and-play network hardware, automated service configuration, and automated, visualized O&M to solve problems with traditional VPN services.

Huawei's CloudVPN redefines enterprise interconnections. For operators, it greatly simplifies service deployment. For enterprise customers, it provides convenient and flexible service options with on-demand interconnections for maximum convenience.

The architecture

The architecture comprises four elements:

The **network infrastructure layer** includes hardware such as virtualized and physical customer premise hardware (CPE) and firewalls. These support physical interconnections between enterprise tenants and cloud DC elements (CloudCPE).

The **control layer** leverages a unified controller called Agile Controller (AC), which provides control and service configuration functions for CPE and DC hardware.

The **orchestration layer** enables E2E cross-overlay and WAN controller orchestration, including orchestrating tenant resources on the enterprise and cloud sides and orchestrating CPE and virtual network function (VNF) NEs. Tenant and operator

control commands are converted into a language that the unified controller can read, and then issued to the bearer device.

The **user interface** includes a service portal and mobile app. It provides a unified graphical interface for tenant and operator administrators, and supports self-service customization on CloudVPN services.

To maintain openness, the southbound and northbound interface interconnections between each layer use open protocols such as RESTful and NETCONF.

The industry's only complete E2E solution

Huawei is the only full-service provider that can integrate different components from an e-commerce platform, mobile app, orchestrator, SDN controller, NFV Infrastructure (NFVI) to CPE, vCPE, and vNGFW. We can quickly provide operators, MSPs, and enterprise customers with a complete customer experience to quickly respond to market opportunities and attract users.

The core component of Huawei's CloudVPN solution is the SDN controller. Unlike other vendors that provide non-integrated products, our AC is a full-scenario unified controller that supports unified control on the enterprise Managed LAN, Managed VPN, Managed VAS, and public cloud access. AC enables E2E resource allocation and automated deployment, providing one-stop interconnection and VAS for enterprises.

For the carrier market, the unified architecture dynamically integrates internal network cloud management, VPN services, VAS applications, and public cloud solutions, providing operators with a complete solution for developing B2B services.

For the enterprise market, lightweight solutions integrate cloud management into the SD WAN and VAS to meet the requirements of enterprise applications, setting the solution apart from competitors' separate solutions.

Full-scenario cloudified interconnection and VAS

CloudVPN can be applied in more access scenarios than any other solution in the industry, because it provides the most complete range of CPE types, including fat and thin CPE, and interface types, including G.fast, PON, and hybrid access.

It also offers the highest-capacity secure virtualized VAS in the industry, with over 12 types of VAS: NAT, access control, SSL VPN, application control, web filtering, anti-virus and anti-intrusion, anti-DDoS, anti-leakage, anti-APT, compliance, load balancing, and WAN acceleration.

The solution also enables minute-level rapid service scheduling via the orchestrator and automated service combination. It has the capability for virtualized, secure, and flexible capacity expansion up to 2.5 T. These benefits provide users with simple, quick, and low-cost interconnections and VAS.

Fully open system maximizes collaboration

Unlike competitors' closed systems, Huawei's

Huawei is the only full-service provider that can integrate different components from an e-commerce platform, mobile app, orchestrator, SDN controller, NFV Infrastructure (NFVI) to CPE, vCPE, and vNGFW

CloudVPN solution was developed based on the principles of openness and collaboration. Each layer of CloudVPN is based on standard interfaces so third-party connections can be selected, including VAS, NFVI, MANO, e-commerce platforms, and CPE.

Commercial value

Huawei's CloudVPN solves the problems with traditional enterprise VPN solutions: It cuts average service provisioning periods from several weeks to minutes; migrating network functions and VAS to the cloud enables flexible enterprise services; and integrating cloud and pipe services allows operators to provide one-stop ICT services for enterprises.

For enterprises

Rapid service acquisition is possible through the self-service purchase of devices and services, plug and play deployment, remote hardware configuration and maintenance, and E2E whole-process automation. Service provisioning for traditional solutions is slashed from 30 days to 20 minutes, enabling rapid enterprise VPN service provision.

Flexible service selection via CloudVPN's e-commerce-style platform enables enterprise customers to purchase enterprise interconnection services and VAS on-demand, avoiding the high costs of a service package.

One-stop ICT services are provided by the solution's one-stop, online provisioning of VPN and VAS for enterprises on the integrated cloud and pipe.

For operators

Rapid service provisioning and lower O&M costs are made possible with the streamlined processes offered by CloudVPN, with automated service deployment and configuration. Plug-and-play hardware reduces the need for on-site service and labor costs. Complex functions are migrated to the DC, enabling centralized O&M, further reducing the need for on-site services.

Increased cloud service competitiveness and revenue through the cloud and pipe services via ICT service synergy provide flexible VAS, increasing revenues for operators.

The wrap up

The SDN controller and CloudCPE are deployed in the DC. Users are able to purchase devices and services and upgrade services on the self-service app. Thin CPE with plug-and-play, zero configuration, and automatic registration functions are deployed in an enterprise's headquarters and branch offices. Video and telephony services are then immediately available in headquarters and branch offices once the controller service is issued.

In addition to network interconnection, CloudVPN also provides cloud VAS such as a firewall, IPS, NAT, and SSL VPN. Users can activate service functions in real time on the service portal or mobile app. Service functions become effective immediately, providing a true "Any Service Online" experience for enterprise users.

Four challenges, three phases, and a one-stop transformation solution

For operators, network transformation has four main challenges in its three stages of planning and design, integration and delivery, and O&M. Huawei's one-stop solution enables operators to build a powerful infrastructure with SDN and NFV to overcome challenges in multi-vendor integration and management, carrier-grade reliability, smooth evolution, and rapid fault demarcation and location.

By Zhang Lei, Yu Zhengang

High priority

The *dumb pipe* threat facing operators from OTT players is exacerbated by the nature of traditional networks. They slow carriers' response to changes in user needs and are poised to waste decades' worth of investment. Open, decoupled networks can save money through better resource utilization and simpler O&M, and save time by enabling rapid service innovation and faster TTM. Telcos can also enjoy more clout in the industry through increased pipe efficiency and by building extensive industry ecosystems.

SDN/NFV is the network transformation enabler, but it's tough to implement. Multi-vendor integration and management, carrier-grade reliability, smooth evolution, and rapid fault demarcation and location all complicate transformation.

One-stop shop

The right partner can help operators analyze business demands and objectives, develop a service architecture blueprint, and take on responsibility for unified network O&M.

To this end, Huawei built its Cloud Open Lab, ICT Support Unified Platform (ISUP), IntOps for integrating operations, and Network Integration Cloud Service (NICS) tools for better efficiency.

The Huawei services based on these solutions are:

NFV and SDN Integration
NFVI Integration
IES Integration (IES = Infrastructure Enabling System)
Consulting Services
Customer Support
Managed Services
Training

These combine to form Huawei's one-stop, all-in-one solution.

The three phases

Planning and design: Huawei and the operator jointly benchmark business and services, and analyze the operator's market position, business vision, and current network situation. They then develop a timeline for deploying DCs and services for maximum ROI, and formulate a plan for smoothly evolving from the old network to the new one.

Huawei ensures carrier-grade service SLAs and considers Virtualized Network Functions (VNF), integrated telecom cloud, and the IES control platform when designing telecom clouds. As part of this, VNF

indicators are mapped onto the integrated telecom cloud and the control platform. This will guide redundancy planning for the integrated telecom cloud and the development of management policies for resource scheduling on the control platform. The goal is to ensure high reliability when deploying multi-vendor hardware in decoupled layers.

Integration and delivery: Huawei will match roles and carry out refined management on roles based on ISUP-defined workflows.

Using the Cloud Open Lab allows pre-integration and the verification of multi-vendor products in advance. This ensures consistency between the ports, protocols, parameters, and data formats of different vendors' products, solving compatibility problems in the lab. By enabling interoperability, project delivery cycles are shortened and on-site integration is simplified.

O&M: Huawei employs the multi-vendor SPOC (Single Point of Contact) maintenance and management services to ensure high service availability based on the principle of restore, then resolve.

An MSUP (Managed Service Unified Platform) for converged ICT network architecture sorts and optimizes organizational architecture models.

During actual O&M, daily monitoring methods and active fault injection, sub-health detection, fault isolation, and cross-layer fault demarcation/location capabilities are dynamically combined. This enables comprehensive network health evaluation that improves network quality, while compatibility management ensures network stability.

In each phase, Huawei continues to build one-stop network transformation service capabilities in SDN/NFV, and completes pre-integration verification using Cloud Open Lab under an extensive ecosystem.

Converged O&M capabilities ensure the stable operation of operators' SDN/NFV network services and support successful network architecture transformation with end-to-end, one-stop services.

Ooredoo's UNIFY 2020 strategy and Qatar pilot

Under UNIFY 2020, Ooredoo wanted to transform its network into a next-gen infrastructure and provide a digital user experience through simpler, more agile network architecture.

The operator planned to transform its traditional service delivery model through SDN/NFV to, according to the company, "Give any new service to any consumer or business customer anywhere in days at low cost."

Ooredoo carried out a pilot in Qatar, successfully verifying its VoLTE service using NFV provided by Huawei's one-stop network transformation services. For the project, Ooredoo adopted a multi-vendor approach involving Huawei, VMware, and HP. Integrating a variety of service modules

and solutions from different vendors is complex and difficult. Huawei acted as the project's Prime System Integrator (PSI), integrating and managing multiple vendors' systems into a unified NFV infrastructure.

Huawei delivered its one-stop network transformation service solution comprising integrated third-party infrastructure, Cloud OS, and Huawei's CloudIMS application. Integration and deployment during the project were based on the design blueprint of converged ICT infrastructure. A unified management platform was used to enable elastic IT resource sharing, and the co-deployment of multiple tenants and service domains.

E2E deployment involved integrating and deploying multi-vendor architecture on different layers, including coordinating and streamlining VNFs and the integrated telecoms cloud platform. Ooredoo also used Huawei's Cloud Open Lab for testing and verification to overcome on-site integration and testing issues and enable rapid, agile integration.

With Huawei's assistance, Ooredoo completed the objectives of its UNIFY 2020 strategy in the Qatar pilot, building its cloud DC in less than two months, which gave the operator the ability to share data center resources on demand. This greatly boosted resource utilization, and ensured Ooredoo could complete CloudIMS deployment in just three hours, thus ensuring extremely quick VoLTE deployment. Ooredoo also implemented cross-DC disaster recovery on management clusters and the cross-DC long-distance hot migration of virtual machines. This would enable uninterrupted services, ensuring 99.999 percent availability for Ooredoo's telecom services.

Moreover, the operator accumulated experience and models that it could replicate on its subsidiary's networks. Thanks to the project, Ooredoo also became the first operator in the Middle East to offer subscribers VoLTE services based on virtual infrastructure.

The Deputy CEO for Ooredoo Group, Waleed Al Sayed, explained the significance of leveraging existing infrastructure for VoLTE services: "We've designed an infrastructure that can evolve and grow using the latest cutting-edge technology, enabling Ooredoo to be the first operator in the region to introduce VoLTE services for our customers. The successful implementation and deployment of these services contributes to Ooredoo's leadership in the era of global ICT convergence."

Huawei and Ooredoo awarded GTB Innovation Award for the UNIFY project

Ooredoo and Huawei were jointly awarded the Infrastructure Innovation Award at the Global Telecoms Business (GTB) Innovation Awards 2016 ceremony in London on May 26, 2016. The award was in recognition of Project UNIFY: Transforming Infrastructure with NFV.

Salem Mohammed A. H. Almarri, Ooredoo's Senior Director for Core Network, and Zhai Zhongcheng, Director of NFV Integration Services at Huawei Global Technical Service, accepted the award together.

Telecom Argentina

Transforming into 2020 with cloud

By Akik A K M Fazlul Haque, Core Network Marketing Execution, Huawei

With mobile penetration hitting 140 percent by early 2016, Argentina has one of the most dynamic mobile markets in Latin America and the third largest after Brazil and Mexico. Its mobile penetration rate for unique subscribers is 90 percent, comfortably beating out Europe at 85 percent, the US at 80 percent, and the regional average of 68 percent.

Active in fixed services, personal mobile services, and Nucleo mobile services, Telecom Argentina is the largest integrated operator in the nation of just over 44 million, generating the highest ARPU value and income in the market. Its revenues are also on an upward trajectory, increasing by nearly

49 percent from 27.3 billion Argentine pesos (US$1.71 billion) in 2013 to 40.5 billion in 2015.

Time to grow

Because market saturation has flattened out subscriber growth, most development over the next five or six years will come from migrating existing subscribers to mobile broadband services on 3G and 4G .

Argentina's adoption of 4G has been the fastest in Latin America, with GSMA Intelligence estimating that 3G and 4G subscriber penetration in the nation will rise to 56 percent of the population by 2020, up from 37 percent at the close of 2015.

Moreover, new growth opportunities exist as the ICT ecosystem expands. GSMA Intelligence analysts estimate that the CAGR for cellular IoT connections in Latin America will increase by 25 percent to hit 62 million by 2020. Moreover, Buenos Aires has set its sights on becoming one of the top 10 smart cities in Latin America, with operators planning to collaborate on projects covering transport, mHealth, and energy optimization over the next five years.

All on cloud by 2020

The increasing competition, huge rise in network demand, business opportunities, and potential in the local market are all factors that Telecom Argentina understands. The result was the operator's five-year transformation plan up to 2020 to cement its position as the leading fixed and mobile operator in Argentina.

Placing NFV front and center, the strategy's objectives are as follows:

Create a more agile, simple, efficient, and automated network to complete ICT convergence and digital transformation by 2020.

Implement an E2E deployment plan for cloud-based VoLTE, VoWiFi, and VoBB along with Rich Communication Services (RCS).

Provide a converged user experience through FMC.

Deliver the optimum MBB solution to subscribers.

Offer Communications as a Service (CaaS) to encourage service innovation and monetize network capabilities.

The pain points

Identified by Huawei in conjunction with a service provider, Telecom Argentina suffered from various ailments:

Complex network, tough maintenance, and high OPEX: The legacy network ran too many MSCs, three different hardware platforms under MSC pools, and a high number of low-performing, power-hungry MGWs. A huge footprint compounded by sky-high CAPEX and OPEX were long-term burdens for Telecom Argentina, with too many network elements and a complex network complicating maintenance.

Because market saturation has flattened out subscriber growth, most development over the next five or six years will come from migrating existing subscribers to mobile broadband services on 3G and 4G

Restricted expansion: The operator's main vendor used a high number of proprietary interfaces, refusing to dock with other manufacturers' equipment and thus restricting expansion. The vendor's TTM was slow and it couldn't keep pace with demand, offering poor evolution capabilities to ICS, FMC, VoLTE, and cloud, which crippled Telecom Argentina's vision for the future.

Network development with Huawei

Successful trials led Telecom Argentina to accept the Huawei proposal for digital transformation by 2020.

The project comprises three central and eight edge data centers (DC), with Huawei's NFV solution installed in phases. The infrastructure layer of the DCs consists of the Huawei COTS FusionServer E9000 with Openstack-based Huawei Cloud OS FusionSphere deployed on top. The Huawei MANO is responsible for service orchestration, VNF deployment, and VNF scale-in/out.

Huawei enabled VNF with its CloudIMS, CloudEPC, and CloudDRA solutions installed in an E2E full cloud-based architecture. Three central DCs host control plane elements to keep costs low, while edge DCs host data plane elements to improve user experience. The three central DCs form a network-wide disaster recovery solution for all sites, and fall under the unified management of EMS/MANO.

CloudIMS and CloudEPC were deployed for VoLTE, native VoWiFi, and RCS in the initial phase, which was followed by the mass commercial launch of VoLTE plus VoWiFi and VoBB migration. ICS and IMS roaming, convergence conference, unified communications, and CaaS will become effective in successive phases.

All core solutions are NFV-based, and were deployed by the end of 2016.

The right vendor

Telecom Argentina chose Huawei for this project based on its cutover experience, flexible commercial solutions, and the following benefits that Huawei's R&D and TSD teams could offer:

Raising capabilities through abundant multimedia services: Huawei's IMS solution allows Telecom Argentina to quickly launch new services, including video and enterprise communications services as well as voice, which will raise ARPU by attracting high-end customers. Rapid and diverse service rollout will also increase the operator's competitiveness.

Easy maintenance, simple network structure, and far lower TCO: Simplifying the tracing of E2E signaling and unified SingleOSS also simplifies maintenance by locating faults up to 16 times faster, while E2E media tracing helps maintain voice quality. The Huawei solution contains fewer nodes, which greatly simplifies network structure with real time geo-redundancy, and slashes O&M costs.

Full cloud transformation with a carrier grade solution: The Huawei solution is based on fully cloud-based architecture. VNF architecture is optimized and reconstructed by using cloud to support three-layered software architecture comprising load balancing, distributed databases, and stateless service processing units. Moreover, it can complete elastic scaling in a few seconds without interrupting ongoing sessions. The new architecture also introduces automatic services and orchestrates resources to enhance the flexibility and elasticity of the entire system. In addition, 99.999 percent carrier-class reliability on cloud networks is achieved through innovations like KPI-based health checks, auto-recovery, and disaster tolerance spanning multiple DCs.

Migration to all-IP: Huawei's cloud based IMS solution will help Telecom Argentina deploy an IP-based fixed voice service. Migrating to all-IP architecture allows services like VoLTE and VoWiFi to be easily deployed, raising the operator's game from voice to dual HD underpinned by an E2E security solution. FMC services will streamline the boundary between fixed and mobile services for a converged user experience.

Huawei is an active participant in NFV standards organizations and driving NFV maturation and commercialization around the world. Huawei's CloudCore and CloudEdge solutions have completed extensive Proof of Concept (POC) testing across multiple continents. Huawei is a leading NFV solution provider with the highest number of deployment cases, winning 87 commercial NVF contracts in 1H 2016 alone.

In 2017, Huawei will continue to help operators build their own agile, open, and flexible cloud networks, promoting the positive development of the global mobile industry.

Getting close to you: MEC@CloudEdge

Mobile Edge Computing (MEC) architecture positions network functions and third-party applications at the network edge, enabling application, content, and network orchestration. Processing services closer to the user also provides users with better-quality services.

By Yin Dongming

User expectations on service experience have risen in tandem with wireless network speeds. Meeting this higher demand requires a new kind of architecture and service delivery method – one that can deliver more exciting services.

This new architecture is MEC, service solutions for which were demonstrated at MWC 2016. Huawei's MEC@CloudEdge is a 5G-oriented MEC solution.

From flat to edge

Mobile networks have evolved with less service processing nodes and delayered architecture. In the 2G era, users had to pass through the base station, base station controller, SGSN,

and GGSN, before connecting to the Internet, making already sluggish Internet speeds even slower.

By the time mobile networks entered the LTE era, network architecture was largely delayered and Internet access had been simplified into a two-hop system. To access Internet services, a user could connect straight from the base station to the core network gateway, greatly improving experience.

However, we're now in the 5G era of ultra-low latency, ultra-high bandwidth, and large-scale IoT service requirements from different industries, requirements that current network architecture cannot meet.

Low latency at the network edge

Since mobile networks first supported data services, each new generation of mobile technology has aimed to improve network throughput to enhance user experience. As throughput has increased, Internet connection speed is no longer a bottleneck for experience, with latency becoming the key factor affecting user experience.

Research on the application side shows that, for high quality, video services have extremely high latency requirements. For example, augmented reality (AR) and virtual reality (VR) video services require latency of below 20 ms, with latency any higher for the latter causing VR sickness. A service objective tied in with 5G is E2E latency of 1 ms to support the demands of services such as Internet of Vehicles (IoV) and industrial control.

However, current mobile technology can't minimize latency. With LTE, for example, air interface throughput is increased tenfold, but E2E latency is improved only threefold due to sub-optimal network architecture.

Although LTE networks possess two-hop flat architecture, the base station and the core network are often separated by hundreds of kilometers, with multiple aggregation and forwarding devices deployed in between. Add unpredictable congestion and jitter to the mix, and it's impossible to ensure ultra-low latency on LTE networks.

To support services with very strict latency requirements, it's necessary to move network functions and service processing functions to the edge of the network, closer to the user. This reduces the number of intermediate layers, enabling low-latency service processing.

Content localization for ultra-high traffic

Current mobile networks were designed for voice services. Network architecture adopts a tree structure, where services are converged at central nodes to be processed. This allows for frequent service concurrency and transmission efficiency.

But, with MBB services, this kind of network architecture can encounter problems. For example,1,000 users watching a 10 MB viral video would produce 10 GB of network traffic because the content is re-transmitted from the Internet to the mobile network 1,000 times. Therefore, 99.9 percent of the network bandwidth used is wasted. So, caching the video in an edge node close to the access point would save the carrier a huge amount of transmission bandwidth.

As air interface throughput is greatly increased and network traffic continues to grow, network-side inefficiency will increase, making content localization essential.

What verticals need

Mobile broadband networks are becoming the basic platforms for office work and marketing, with companies expecting customized networks to meet their specific needs. Some, for example, want data access to the private cloud to be completed within their enterprise campus networks to ensure mobile office security, meaning that network functions must be deployed on the campus network and support local breakout. Another example

In Huawei's 5G-oriented MEC solution, MEC@ CloudEdge, applications, content, and some MBB core network service processing and resource scheduling functions are deployed at the network edge, closer to the access point

is the idea of smart billboards proposed by a Korean operator for smart crowd analysis based on network data – the local content changes to increase the advertising conversion rate. This kind of service requires a localized, open network platform.

5G edge cloud with MEC@ CloudEdge

In Huawei's 5G-oriented MEC solution, MEC@CloudEdge, applications, content, and some MBB core network service processing and resource scheduling functions are deployed at the network edge, closer to the access point. This enables both services to be processed closer to the user and also application, content, and network orchestration. As a result, users are provided with reliable, ultimate service experiences.

MEC@CloudEdge: Deployment scenarios

Experience and efficiency must be balanced for deployment. Deploying the solution closer to the base station side requires fewer intermediary nodes, which improves experience. But, it also means there will be fewer users accessing the node, reducing utilization.

Deployment location needs to consider scenario-based service requirements. For example, some enterprises want private cloud data access to be completed within their enterprise campus networks, requiring the solution to be deployed within their campus network. For sports stadiums that provide live playback, interaction services, online purchasing, and location services for match-goers, the solution would need to be deployed in the stadium.

Based on service requirements and resource efficiency, these demands mean that MEC@ CloudEdge should be deployed between the edge of the metropolitan area network (MAN) and the base station. This might include central offices (CO) and a number of specific venues and campuses.

MEC@CloudEdge: Main functions

To meet service requirements, MEC@ CloudEdge offers the following main functions:

End of the user plane: runs core network functions such as billing and policy, and meets requirements for billing, monitoring, mobility, and O&M.

Local Breakout (LBO) for services: uses LBO functionality to support localized content and application processing, so the user can directly access local content via MEC without routing to the central core network gateway.

Third-party application registration and management: supports third-party application integration, including registration, discovery, and unified management on tasks like resource scheduling and health checks. This allows network functions to be expanded and third-party services to be customized, as well as service traffic and content awareness and orchestration, so services can be optimized to improve experience.

Network function sharing: provides an open platform for services to be customized for verticals and enables flexible third-party service deployment. With an open platform, internal network capabilities are shared, making seamless integration with third-party services possible.

MEC@CloudEdge: Solution structure

MEC@CloudEdge is based on Huawei's CloudEdge platform. It can be deployed on the same hardware, with third-party applications based on general servers. The solution can share network functions to support new service innovation for operators, and enable on-demand modular deployment on the control, user, enabling, and management planes.

MEC@CloudEdge: Key technologies

MEC tech used to be constrained by platform sharing technologies and commercial factors before actual deployment. But now, the maturity and application of NFV technology has prompted the industry to develop standards for MEC and carry out R&D on MEC solutions.

MEC@CloudEdge's main enabling technologies include:

NFV and cloud technology to support multi-tenancy: NFV technology supports multiple tenants on the MEC@CloudEdge. It also enables co-platform deployment and unified resource management on gateway functions and third-party applications. However, as the deployment location is lower using NFV, node capacity is relatively small. This means using NFV alone cannot ensure the reliability and performance provided by large-scale DCs.

Therefore, it's necessary to introduce cloudified software architecture on top of NFV, so software functions can be decoupled and deployed as layers based on the properties of the different capabilities. This enables high reliability, high flexibility, and high performance when resources are limited.

CU separation for flexible deployment of network functions: When MEC@CloudEdge is deployed close to the access point, core network gateway functions are distributed at the edge of the network. This creates a large amount of interface configuration, connection, and commissioning. Thus, the core network's control plane and user plane must be separated to allow the gateways to be flexibly deployed and to simplify the network.

Separating the Gateway CU strips away the complex control logic of the gateway. Gateway functions are retained on the traditional central gateway or integrated into an integrated control plane, lowering deployment costs and resolving problems with circuitous signaling routes and the burden on the interface.

Gateway CU separation first requires making the functions lightweight and stripping away complex control logic functions. Next, the basic core functions that are retained are modeled, and the common forwarding plane models and object-oriented interfaces defined. The forwarding plane is then programmable with excellent scalability. Once the complex service functions are stripped away, lightweight configuration is implemented to support one-click deployment.

Service awareness and smart orchestration: To enhance user experience, MEC@CloudEdge supports real-time service awareness and intelligent experience optimization. When, for example, wireless network quality degrades, MEC@CloudEdge can sense the user's video bit rate and send the traffic to a video optimization module, where the video stream is re-encoded, ensuring smooth video for the user.

As MEC is deployed on mobile networks, a number of exciting new functions for work and leisure will emerge. These include MCDN-based HD video experiences; AR/VR-based mobile games; LBS marketing; and secure, reliable LBO-based enterprise mobile office; smart stadiums based on MCDN and open platforms; and traffic assistance systems for IoV. These new technologies will transform life in ways we cannot yet imagine.

All Cloud starts at the core

For operators, full cloudification should start with hardware, before completing network cloudification in phases and then finally transforming service and operation systems. Because core networks process real-time applications, cloudifying core networks is the logical first step.

By Deng Ao

The latest *Heavy Reading* survey shows that some 96 percent of operators plan to cloudify their networks. Huawei's All Cloud strategy aims to help operators build agile, intelligent telecom networks through the cloudification of devices, networks, services, and operations using NFV, SDN, and cloud computing technologies.

These agile, intelligent networks will enable global scheduling, elastic scalability, flexible architecture, fully open capabilities, and fully automated O&M. Operators will be able to achieve full cloudification and provide a ROADS user experience: Real-time, On-demand, All-online, DIY, and Social. However, operators face

complex network architecture and huge legacy networks. So, on this journey of a thousand miles, where should operators take their first step?

The start

For operators, the process of full cloudification and a ROADS experience should start with hardware and applications, areas where operators are strong. Then, network cloudification should be completed in phases using agile SDN networks to connect different kinds of applications in the cloud. With this upgraded infrastructure in place, operators should then transform their service and operation systems to boost service innovation, development, and deployment, and also O&M.

Operators are strong in real-time applications, including voice and video, and they have an advantage as long as there's a requirement for real-time services. And because the core network is the processing center of real-time voice/video applications, cloudifying core networks is the best first step.

The Current Analysis Q4 2015 carrier survey reports that of the eight main first-step cloudification scenarios, 50 percent involved cloudifying core network services and 87 percent of operators were considering 4G HD VoLTE and VoWi-Fi for the next 12 months based on cloudified IMS and EPC.

An agile cloud core

NFV will change infrastructure and deployment methods, which in turn will affect service SLA and network O&M. In their *2013 Network Functions Virtualization – Introductory White Paper*, ETSI NFV Industry Specification Group described nine major challenges facing telecom network cloudification, including performance, reliability, and automation.

To provide carrier-grade SLA for real-time voice and video communication services on cloudified core networks, these issues must be solved.

Ultimate experiences for real-time services in any scenario

Unlike traditional core networks, cloudified core networks must provide carrier-grade service SLA on low-spec, general hardware and also meet the requirements of IoV, industrial control, other low-latency future services, and high-traffic services like AR/VR and 4K video, which have even higher demands on latency and traffic.

Agile service customization and new service innovation capabilities

As the telecoms industry expands from people-to-people communication services to large-scale IoT and vertical industry services, a wide variety of service application scenarios will emerge that have very different requirements on networks. The key demands of future services on cloud core networks will be to support on-demand service customization with limited investment and network resources; enable the seamless integration of operator network capabilities such as voice, QoS control, location data, and third-party services; and accelerate service innovation.

Achieving intelligent and automated O&M

The ICT era has seen the rapid emergence of personalized services, and now there are too many to handle manually. Service awareness-based network automation and intelligent O&M are therefore new industry trends.

Huawei Cloud Core Network

Huawei offers a full series of cloudified core network products, including CloudIMS, CloudEPC, CloudSDM, CloudDRA, CloudPCRF, and CloudSBC, and the new component MANO (Management and Orchestration).

The four key features of Huawei Cloud Core Network are:

Open, fully optimized network construction: Huawei Cloud Core Network features open architecture, with all three layers completely decoupled for integrated deployment with general hardware, the cloud operations systems of multiple vendors, and third-party virtual network functions (VNF). Operators can leverage the solution's open architecture for on-demand selection, partnerships with third parties, and flexible deployment, and to minimize network construction costs.

Distributed, cloudified software architecture for carrier-grade capabilities: In addition to software and hardware decoupling, Huawei Cloud Core Network improves resource utilization and service elasticity through leading distributed, cloudified software architecture, ensuring carrier-grade capabilities that are independent of hardware infrastructure. At the same time, the control and user planes can be separated, supporting the flexible, on-demand deployment of network functions. Control plane functions are deployed centrally, simplifying the network, while user plane functions can be deployed at the edge of the network, closer to the user, for the best service experience.

Service awareness-based intelligent O&M for the best service experience: With various innovative technologies, Huawei Cloud Core Network supports health monitoring and fault self-healing based on service KPIs, smart and differentiated service chain orchestration, service awareness-based dynamic application deployment, and a series of smart tool platforms like performance evaluation and E2E fault identification/location tools. These features enable on-demand resource orchestration, on-demand dynamic deployment of services from the center to the edge, rapid fault recovery, and self-healing. O&M is thus smart and oriented to service experience.

Atomic-level network capabilities for one-stop opening and orchestration to promote service innovation: By flexibly orchestrating atomic-level network capabilities, differentiated network capabilities can be quickly assembled on a physical cloud core network, meeting the experience demands of different industries and services. A one-stop network capability opening platform can open communications capabilities such as voice, video, QoS, computing, storage, and network resources. For new service innovation, Huawei Cloud Core Network provides an integrated environment and management platform covering the entire service lifecycle, including development, testing, launch, and operations. This supports immediate service development and provisioning, and promotes service innovation.

As of Q4 2016, Huawei Cloud Core Network has been deployed in over 130 commercial networks, including networks operated by Deutsche Telekom, Vodafone, Ooredoo, and China Mobile, all of whom have formed strategic deployment partnerships with Huawei.

Huawei Cloud Core Network and its partners are poised to ramp up business value for customers with innovative services and drive All Cloud transformation.

A new silver lining for MBB when networks go cloudy

Mobile Internet has enabled OTT services to flourish, breaking the original value chain and creating massive challenges for telcos. Because current networks are no longer up to the task of meeting the varied needs of different verticals, cloud networks can help operators expand business boundaries, create new business models, and build open ecosystems.

By Zhang Xi

IoT Packet Core

IoT is set to become a key blue-ocean market in the future, with Narrowband IoT (NB-IoT) as the main enabling tech. NB-IoT terminals are near perfect for near ubiquitous coverage: They're inexpensive, consume very little power, and offer Plug and Play functionality.

One NB-IoT application is smart parking, which given today's urban congestion is needed more than ever. In fact, some 30 percent of traffic jams are caused by drivers looking for a parking spot. Intelligent parking systems locate spaces straight away, which drivers can then reserve to avoid driving around lots to look for empty ones.

Huawei offers an intelligent parking solution based on NB-IoT networks. Its main feature is IoT Packet Core, which offers scalable and flexible network support for IoT applications as part of Huawei's CloudEdge solution.

IoT Packet Core provides signal management functionality for low-power and low-cost UE, enhanced coverage, and congestion control. For example, NB-IoT enhances 20 dB more coverage than GPRS, allowing near ubiquitous network coverage and solving the problem of weak signals in underground parking lots. Vehicle detectors based on NB-IoT are plug-and-play, provide a decade's battery life, and are very easy to maintain. The solution also offers carrier-grade reliability and security.

In 2016, Huawei carried out demonstrations of the intelligent parking system with a number of operators in different parts of the world, including Bell in Canada, T-Mobile in Germany, ET in the UAE, Shanghai Unicom in China, and LG U+ in South Korea. At the end of 2016, Huawei started deploying the system commercially for Shanghai Disney in partnership with Shanghai Unicom.

CloudMSE

The data explosion and popularity of smart devices and mobile broadband (MBB) are driving the rapid development of the MBB market. But, services are becoming more complex. With fixed and mobile networks converging, operators are facing more difficulties with profit models, billing, and user experience.

Huawei's CloudMSE solution is based on the cloudification technology GiLAN. The solution provides multiple types of access methods, including GPRS, UMTS, LTE, CDMA, WiFi, and Fix. It offers service-based billing and bandwidth control, service awareness, and a third-party app integration platform for smart service chain. CloudMSE enables integrated operations and management on third-party apps, and flexibly orchestrates the service chain based on user, access type, and OTT service. New services can be quickly launched, helping operators shorten TTM and lower CAPEX and OPEX by solving the management problems on traditional MBB networks.

Intelligent service aggregation platform

Standardized operation models and an outstanding service experience are operators' core competitive strengths. For MBB networks, service usage frequency and loyalty are determined by user experience, which directly impacts operators' earnings. QoE is in turn determined by a range of factors such as the newness, richness, tariff, and access speed of services.

To retain high-value users, deliver diverse and personalized services, and refine pipe operations, more mobile operators are increasing network functions on the Gi interface. These include new services such as header enhancement, transmission optimization, content optimization, content filtering, and ad insertion. Huawei's CloudMSE solution provides a smart services aggregation platform that integrates industry-leading third-party applications and provides

more agile and efficient GiLAN solutions for operators.

Extensive third-party capabilities help build the app ecosystem

Operators can greatly enhance user experience, boost loyalty, and attract new subscribers with VAS, precise pipe operations using the Gi interface data, and functions such as content optimization and acceleration. Huawei's CloudMSE solution integrates industry-leading third-party VAS applications, allowing operators to rapidly deploy VAS solutions, optimize pipeline operations, and improve end-user experience.

The Saudi Arabian carrier Zain wanted to lower its international bandwidth and cut costs by optimizing video traffic so it could offer more competitive service plans. Zain adopted Huawei's CloudMSE video optimization solution, deploying the services aggregation platform and using third-party video optimization modules. This helped the operator reduce bandwidth by 11.57 percent.

CloudUIC

In today's era of rapid MBB traffic growth, operators must extract more value from data services as well as provide pipe bandwidth for connectivity. Better O&M planning and marketing, automated services, and improved support for third-party enterprise applications can all help create new services and income streams.

Based on Huawei's CloudEdge solution, CloudUIC can open network capabilities. It combines and orchestrates various atomic capabilities on operator networks, providing a large number of interfaces that can be invoked by third-party applications. Among these, location and QoS capabilities deliver the greatest value.

Opening capabilities: Digital Footprint

Huawei's Digital Footprint solution integrates MBB network location capabilities for third-party demand, allowing third parties to invoke the services they need via APIs. It collects, positions, and analyzes location data for mobile operators, including location history analysis and real-time location analysis, and opens these up to third parties via APIs. Operators and third parties can then develop new business models for commercial applications.

Opening capabilities: On-demand acceleration

Huawei's on-demand acceleration solution packages operators' QoS resources into APIs and makes them available for Internet applications to invoke. The solution can accelerate OTT services for tens of millions of users on demand without complex PCC configuration or verification on the PCRF. The main value of Huawei's on-demand acceleration solution lies in providing flexible QoS guarantees and easily invoking APIs.

Solutions for verticals

Cloud-based networks cause diverse requirements and new application scenarios to quickly emerge, bringing both opportunities and challenges.

Automated MVNO for operators

Opportunity: MVNO (mobile virtual network operator) is a new option for traditional operators to deploy in specific market segments to respond to competition. By setting up an MVNO subsidiary, operators can develop new services under new brands and adopt more radical market strategies to attract customers without being tied to their original brands or customer bases.

Challenge: MVNOs are separately deployed, and miniaturized equipment is needed to lower costs; different MVNO customers require different versions, features, and O&M methods; and highly stable hardware is needed to provide QoS guarantees.

Enterprise wireless broadband

Opportunity: As LTE technology

Huawei's miniature EPC has enterprise-level ease of use and easy O&M, so it doesn't require installation, configuration, or maintenance

matures and develops, 4G chips and terminals are getting cheaper, and 4G applications are becoming more popular. Operators can deploy LTE small cells and enterprise-level evolved packet core (EPC) inside large companies. Local data services can be accessed via local breakout (LBO), providing the shortest path. This helps reduce the use of valuable EPC backbone bandwidth and network traffic, but it also improves user experience. In addition, SMEs can consider outsourcing office wireless network infrastructure to operators to reduce the amount they have to invest in IT, increase reliability, and enable better indoor coverage to improve network experience for employees.

Challenge: Equipment must be deployable without requiring installation, configuration, or maintenance, and it must be easy to use. It needs to be low-cost to help reduce companies' IT investment burden.

Public safety

Opportunity: Public safety bodies must be able to deal with events like emergencies, civil unrest, traffic accidents, natural disasters, and large public events. To do so, these bodies need to use technology, including information platforms, big data systems, and video surveillance.

Natural and man-made disasters have the potential to damage communications equipment or block it through congestion due to a surge in use. Emergency vehicle-mounted communications systems, including base stations, miniature EPCs, and cluster servers can be rapidly deployed to emergency sites. They allow rescue personnel to communicate and provide clustered voice services within the signal range of the vehicle-mounted base station. The solution ensures the reliability of unified command and dispatch through temporary command centers.

Challenge: Equipment needs to be very reliable so it won't be damaged or rendered inoperable if disaster strikes, and scaled down in size so it can be easily deployed on different kinds of emergency communications vehicles.

Huawei's miniature EPC, aka the Core in a Box, provides 4S functionality.

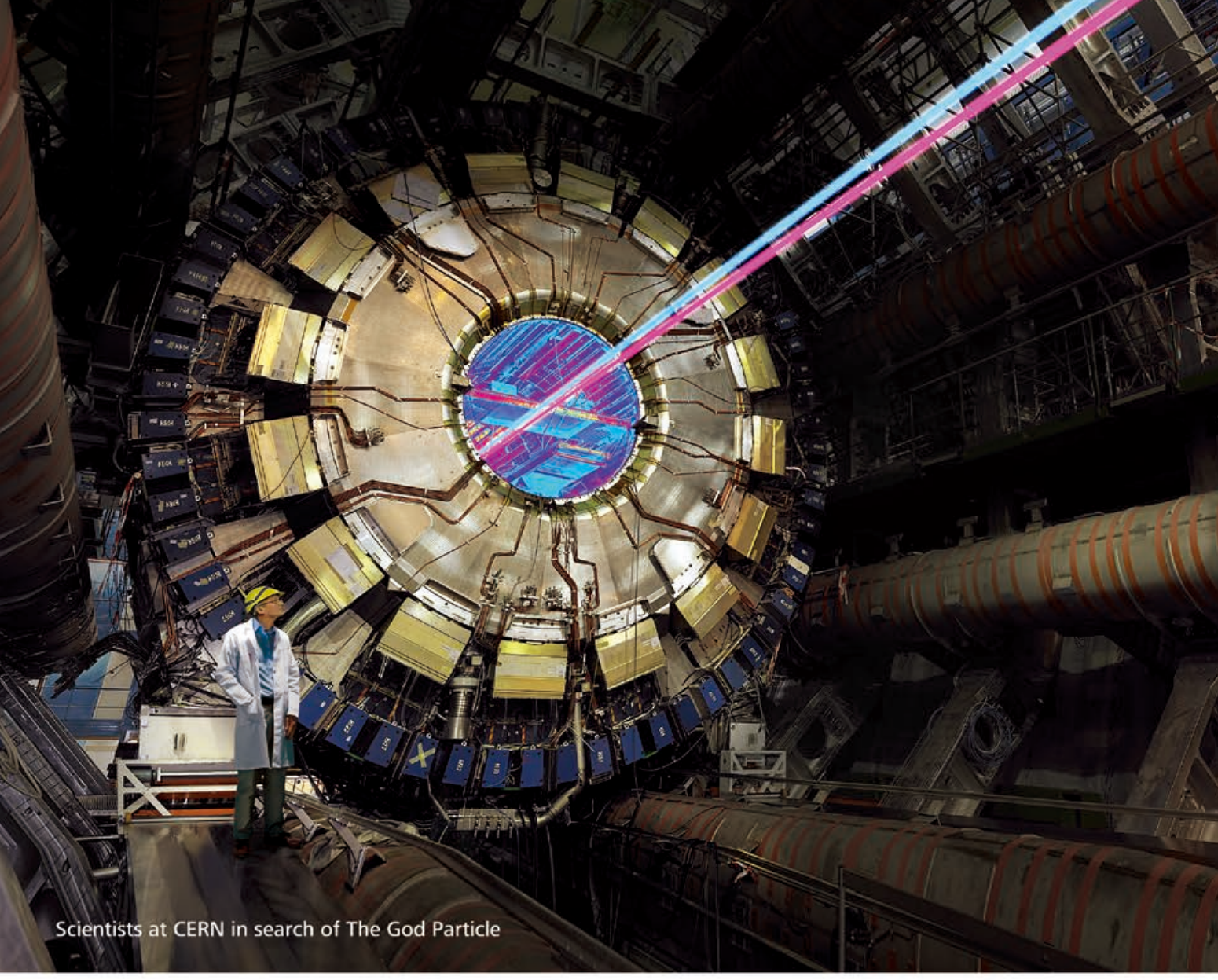
Small: The solution supports 3U and 1U devices that consume little power, leaving a small footprint.

Simple: Plug-and-play doesn't require installation, commissioning, or maintenance, and supports various management options.

Saving: It's inexpensive and doesn't incur maintenance or high energy costs.

Stable: The solution is extremely stable, offering 99.999 percent carrier-grade reliability and high disaster resistance.

Huawei's miniature EPC has enterprise-level ease of use and easy O&M, so it doesn't require installation, configuration, or maintenance. It also meets strict carrier-level downtime requirements and can be rapidly deployed at relatively low cost. As a result, it's perfect for niche and new markets.



Scientists at CERN in search of The God Particle

Decades of patient investment, for a moment of divine clarity

Focus · Persevere · Breakthrough

HUAWEI

HUAWEI

A STEP AHEAD

Revolutionary Smartphone Experience

HUAWEI Mate 9

CO-ENGINEERED WITH Leica

New generation of Kirin 960 processor
EMUI 5.0 with intelligent machine learning algorithm
Groundbreaking solution for ageing smartphone performance

Born Fast Stays Fast

consumer.huawei.com

Product colour, shape, interface and functions are for reference only. The actual product may vary.
Based on normal usage. Product speed depends on actual usage situation.