Leading New ICT, The Road to Digital Transformation.

ICT INSIGHTS

e.huawei.com

Huawei Enterprise

Extra

04/2017
Yue B No. 13154

LEADING NEW ICT

Embrace and Integrate with the Cloud to be a 'Digital Enterprise'

Scan for mobile reading

Building Unified PaaS Architecture for Agile Development

Developing a Scale-Out Data Center Network with the Cloud

Historic Mission and Key Tasks for CIOs in the Digital Era

HUAWEI

Publisher:

ICT Insights Editorial Board,

Huawei Enterprise

Yue B No. 13154

To read or download *ICT Insights* in electronic form, visit
http://e.huawei.com/en/publications/global/ict_insights/
To subscribe to *ICT Insights*, contact the Editorial Board.
Email: ICT@huawei.com
Address: H2, Huawei Industrial Base, Bantian, Longgang, Shenzhen 518129, China
Tel: +86 (755) 28780808, +86 (010) 82882758

Inside

Embrace and Integrate with the Cloud to be a 'Digital Enterprise'

Embrace and Integrate with the Cloud to be a 'Digital Enterprise'

By *Eric Xu*

What exactly is a digital enterprise? What is the purpose of digital transformation? What value will it create? More discussion will be needed across the industry to delve deeper into better answers that are broadly agreed upon.

To become a digital enterprise, a company needs to build ubiquitous connections spanning its people and things and, at the same time, link its employees, customers, partners, and suppliers together. The company's operations should be based on Big Data and Artificial Intelligence (AI). On top of that, it needs to automate its business processes with built-in, real-time decision

Eric Xu

Going digital will be the strategic choice of every enterprise. The key goal during transformation is to provide a ROADS experience for customers, partners, and employees — this is most challenging.

making so as to realize simple, efficient, and intelligent operations. A key goal of this digital transformation is to provide a ROADS experience — Real-time, On-demand, All-online, DIY, and Social — for customers, partners, and employees. This is the most difficult part of the journey, but it's a must, as both enterprise customers and consumers will be expecting a ROADS experience when they buy or use products and services from providers.

Harley-Davidson is a good example. It is one of the world's top brands, with the vision of creating unique motorbikes. Through digital transformation, Harley-Davidson has connected all its production lines and is able to assemble over 1,200 components into a motorbike in just 89 seconds. Its manufacturing assembly lines are precise to the second. Before the company embraced being digital, the whole process from online order to delivery took 21 days. After digital transformation, Harley-Davidson can process all orders online and give consumers the freedom to choose their favorite engine models and colors. Now, the order-to-delivery process only takes six hours.

Digital Targets

For Huawei, we have a target for digitization. We hope that when consumers order a mobile phone at our online store, they can customize the device the way they like. The order will then be automatically transferred to our production line. After the phone is made, it will be automatically shipped to the consumer. Throughout the order-to-delivery process, only manufacturing and transportation will require time, while other procedures will be finished almost instantaneously. When this target becomes a reality, imagine how competitive we will be, and what the operating efficiency and customer experience will look like. Companies that are determined to go digital and ultimately become digital enterprises can greatly enhance their customers' experience, their internal efficiency, and every aspect of their company operations. They are more likely to stand out from the competition. Conversely, companies that fail to take action are likely to fail to compete.

So, the question is, how can companies become digital enterprises? From my point of view, embracing and integrating with the cloud is the key. The idea is to use cloud technologies and mindsets to innovate business and operating models and improve experience and efficiency. Over the past 10 years, Internet companies that were born in the cloud have delivered superior experience and disrupted the business models of many vertical industries. Just imagine, if traditional companies or industries innovated their business and operating models based on cloud technologies and mindsets, then some of them may not be disrupted. By then, it would be the same customers served and the same products offered, but the business and operating models would be redefined with cloud technologies and mindsets to achieve simple and efficient operations at lower cost.

When it comes to embracing and integrating with the cloud, the answer of how to do so is clear. But actually getting there is really difficult. There are many challenges to resolve: the availability of capabilities and talent, interworking between legacy and new applications, and the changes required in processes and software, just to name a few. To tackle all these challenges as enterprises move to the cloud, the solution lies in the cloud itself. Enterprises should explore their implementation strategy from three dimensions: cloud deployment, cloud utilization, and cloud management. Huawei has identified ten issues with enterprise IT and network architecture. The list may not be exhaustive but any company that intends to embrace digital will encounter these ten issues. Next, I will share my observations on five issues that I believe are critical.

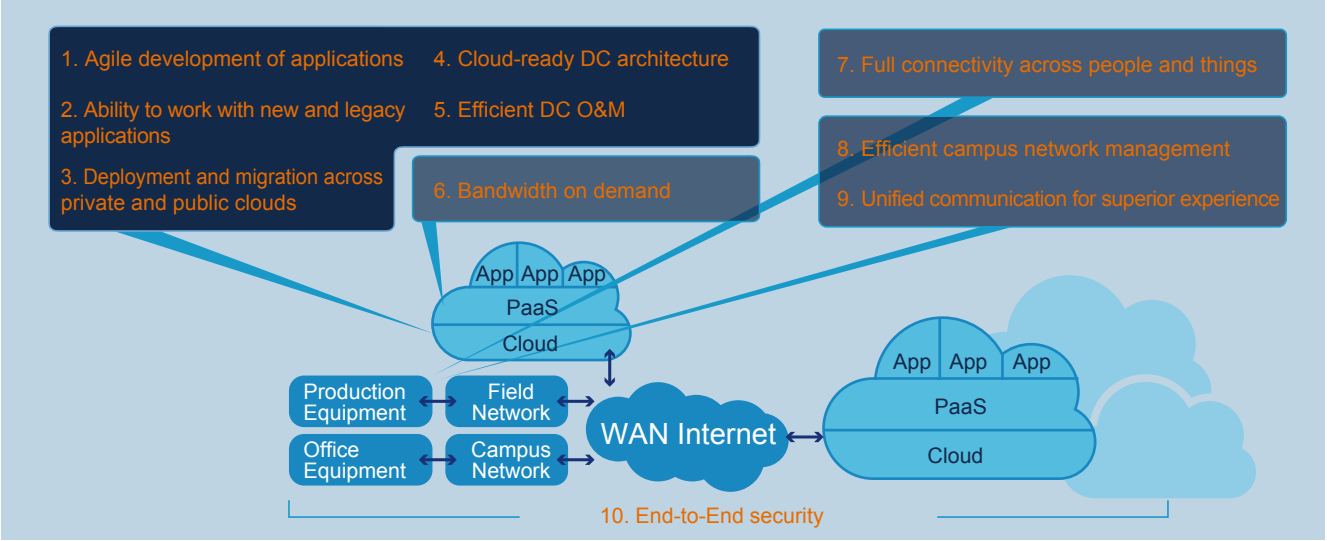


Figure 1: Ten issues for cloud deployment, cloud utilization, and cloud management

Deployment is time-consuming, and automatic scaling is difficult. That's why, over the last couple of years, some large enterprises have thought of developing or introducing a PaaS platform for all common functions. >>

The Big Five

The first issue is agile development of applications, and it's the biggest headache facing enterprises. How can IT application development evolve in sync with business changes? Huawei now has 3,000 in-house staff and many more contractors working on internal IT applications. In 2015, Huawei spent approximately USD 218.3 million (CNY 1.5 billion) on IT outsourcing. This is a huge investment. I've talked with many companies, and their situation is similar — most have a large team, in-house plus outsourced, working on the development of IT applications.

For every IT application brought on board, there's repeated development of the same functions. Deployment is time-consuming, and automatic scaling is difficult. That's why, over the last couple of years, some large enterprises have thought of developing or introducing a Platform-as-a-Service (PaaS) platform for all common functions. However, if every company develops its own PaaS platform, they are just reinventing the wheel, and the architecture of the PaaS ecosystem will become fragmented, quite likely with unsatisfactory performance. I think we'll be better off having a PaaS platform with unified architecture to offer both common, standardized services and industry-specific professional services. With a PaaS platform like this, all enterprises — including software developers and system integrators — can focus their efforts on application development.

The second issue is about security, a critical building block for private and public cloud services. Cloud services are widely seen by many as less secure from several aspects. Most important of all with the cloud, data storage is no longer distributed; it becomes centralized, leading to increased exposure to data breaches and illegal access. Resource-wise, applications used to run on different servers that were physically separated. With the cloud, all physical resources are virtualized, so the security boundary is blurred and the impact of vulnerabilities grows. Building a great wall for segregation might have been enough in the past, but now even virtual machines require layers of defense between themselves. Application is another dimension. We all want rapid and agile application provisioning, but that requires real-time security defense, which is not yet in place. In terms of management, flexibility in resource allocation is certainly desirable and is the biggest advantage of the cloud. But it naturally conflicts with pre-configured privilege management. These are the security challenges in the cloud era.

But it's not all bad news. The cloud also brings new advantages to deal with security challenges. It allows us to adopt a systematic, end-to-end response to security threats through comprehensive and deep analysis. In fact, a public cloud, with its huge security investment and rich portfolio of security services, is surely more secure for Small and Medium-size Enterprises (SMEs), because single SMEs cannot afford to build an equivalent stack. In my opinion, the key to post-cloud security is to build a full-stack security defense system, which covers physical layers, networks, hosts, applications, and data. End-to-end visibility into enterprise security is needed, and that's exactly what the cloud can bring to the table. Big Data and AI will play a role to allow real-time and intelligent risk monitoring and prevention. Last, but not least, it's always important to choose trusted partners to work with.

Data Centers

Data center architecture is the third challenge. Data and traffic volumes are exploding. Existing DCs, with their multi-layer scale-up architecture, can hardly meet current

needs. With existing architecture, DC capacity goes up to hundreds of terabits per second, and there are issues around single points of failure and high power consumption. Maintenance is also a big problem in a large DC with hundreds of thousands of pairs of fiber. These are not the data centers of the future capable of dealing with massive data traffic, storage, and computing. If the notion of the cloud can be used to transform DC architecture from scale-up to scale-out, then petabit/s capacity can be realized and way less fiber would be needed. Such a solution is not in place yet, and I hope the industry will work together, adopt the cloud mindset, and scale-out to replace existing DC architecture.

The fourth issue is bandwidth on demand. As enterprises migrate their data between private and public clouds, or from one public cloud to another, a pressing need is bandwidth on demand. A case in point is Amazon's Snowball, a service that I think the industry should feel embarrassed about. Through express delivery, enterprise customers ship a data-loaded appliance to Amazon, which charges customers USD 200 for every 50 terabytes of data. This physical approach for data transport is neither secure nor convenient, but it is more cost-efficient, as retrieving the same amount of data from the cloud costs between USD 1,000 and USD 2,000. So, if we look from the perspective of enterprises, it is important that carriers provide bandwidth on demand to migrate huge amounts of data fast enough between public and private clouds.

> CIOs have to become leaders in the cloudification of IT architecture. With respect to interconnections, CIOs should play the role of an enabler for interaction between the company and its customers, partners, and employees. >>

The last issue relates to campus network management. Campus networks today are rather complicated, and they need to be managed and maintained by certified professionals. Data configuration has to be done for each piece of equipment. That's the case with Huawei today. We have over 200 branch offices around the world. At every location, we need to assign IT professionals for data configuration. Imagine if we introduced the notion of cloud into campus networks. Network maintenance, policy management, and data configuration could be centralized in the cloud. Enterprises would only need to buy boxes for plug-and-play. Network O&M would be done either in-house or by suppliers or carriers. In any case, centralized and cloud-based management can significantly bring down the operating expenses of campus networks.

Building a digital enterprise requires not only the commitment of the CEO and management team but also renewed thinking about the future role and value of the Chief Information Officer (CIO). CIOs used to be responsible for information only, but now they need to become CI^{3}Os who manage information, innovation, and interconnections. Of these three elements, innovation is the most important. As CIOs have the right ICT expertise and can embrace cloud technologies and mindsets over time, they will be in the best position if they glue technical knowledge to their business. So, this is the first dimension of the CIOs' triple role in the future: driver of innovation in operations and business models. In terms of information, the second 'I', CIOs have to become leaders in the cloudification of IT architecture. With respect to interconnections, CIOs should play the role of an enabler for interaction between the company and its customers, partners, and employees.

Huawei aims to become an enabler and driver of the intelligent world. To this end, we will stay customer-centric, focus on ICT infrastructure, and provide innovative cloud technology. We strive to become an enabler and preferred partner for enterprise cloudification and digitization; actively contribute to the cloud ecosystem; and promote openness, collaboration, and shared success. ▲

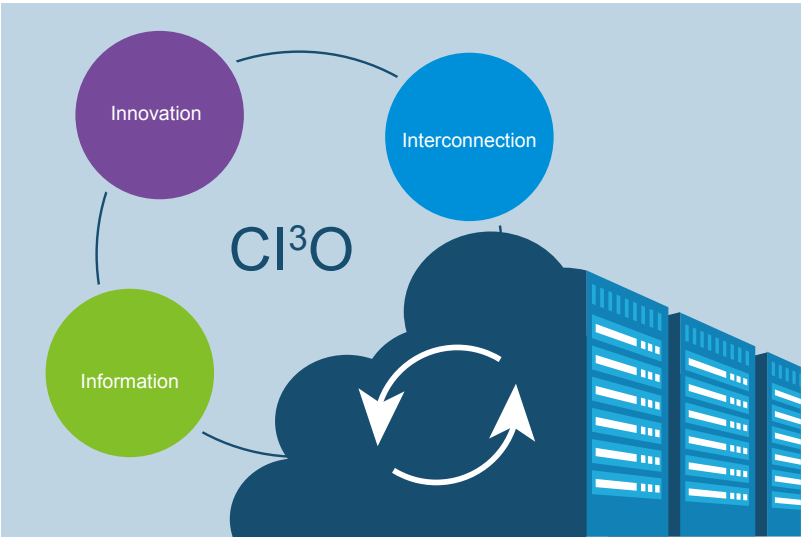
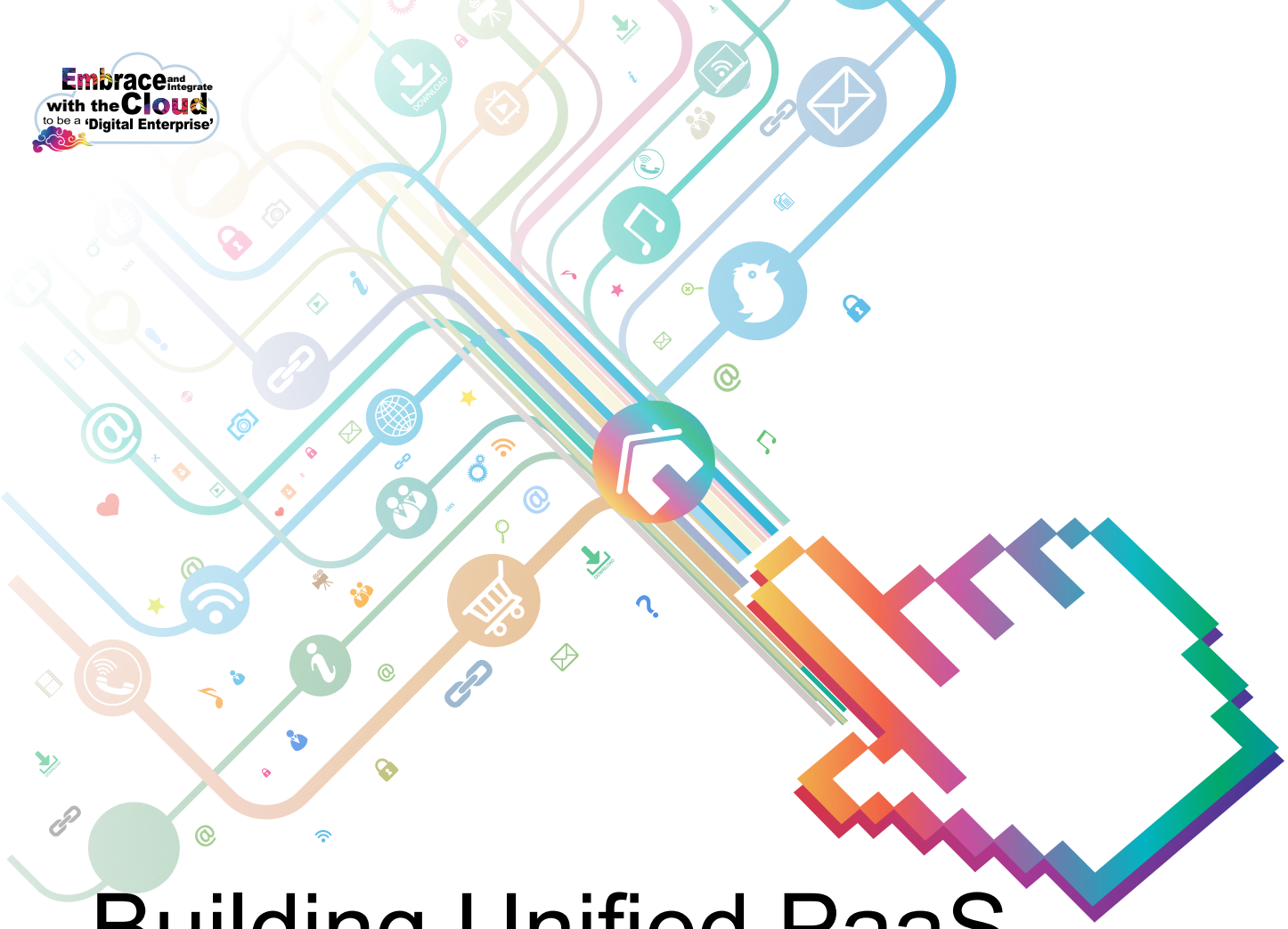


Figure 2: CIOs' triple role in the future



Building Unified PaaS Architecture for **Agile Development**

By *Jack Jia*

Now that we have embarked in an era where information changes at unprecedented speeds, it is essential for us to remain one step ahead of our competitors. How then, do we ensure that we remain both fast and agile in our business innovation and response to our customers? Digital transformation is the one and only answer for enterprises looking to maintain substantial growth, and an agile and efficient IT system is essential to this transformation. All of today's mainstream models for enterprise IT application development are functionality and process based. These models tend to be costly and too cumbersome to meet current requirements, putting enterprises at a disadvantage. The time is ripe for a revolution in IT application development methodology and technology.

Enterprise IT Application Development: Challenges Facing Traditional Models

● Segmented Development Model and Long Time to Market

Most mainstream enterprises have adopted the waterfall development model. This model has several disadvantages. First, business requirements are segmented — business departments raise IT requirements based on enterprise operations demands, and IT departments develop their applications according to these requirements. Second, the IT application development process is a sequential one, which means that progress flows steadily downward through the phases of requirement analysis, solution design, coding, testing, and deployment. Only one or two releases are launched per year. The time-to-market cycle could even be longer if the development process is hampered by cross-departmental barriers. Substantial changes to requirements result in significant delays in delivery or even in a delivery crisis.

The DevOps model contrasts sharply with the waterfall model. It combines development and operations into one process, and is an improvement in many ways. This model allows for trial-and-error tests to be performed quickly on applications, greatly reducing time to market. Having learned from successful Internet companies,

Jack Jia

The core of enterprises adopting agility with cloud computing is to introduce the PaaS platform to achieve application-centric automation and distribution. Unified PaaS, not only in technology and architecture, can effectively support the service and microservice for development and governance, but also play a key role to enable the development process and organizational collaborations.

an increasing number of enterprises have begun to embrace the DevOps model when developing IT applications. However, this change in mindset is far from enough. It is up to us to set up the architecture and build an advanced development model to ensure that the DevOps model becomes the first choice for enterprises around the world.

● Evolving from Monolithic Architectures to Microservices

Over the past decade, enterprises have shifted away from using monolithic architectures to Service-Oriented Architecture (SOA) models, and now to a microservices model.

- **Outdated architecture and low efficiency:** In the monolithic-architecture model, an application's core business logic and defined services, objects, and events are encapsulated in separate modules. These modules and components are packaged and deployed as a whole, leaving the process highly dependent on the language and framework of the application.
- **Tight coupling and one change making all changes:** Although projects using the monolithic-architecture model can be built quickly at an early stage, the inevitable expansion of code and turnover of staff that come later mean that R&D efficiency is subject to rapid decrease. A further disadvantage of the monolithic-architecture model is revealed when adding a requirement of just a few lines of code or fixing a single bug might lead to unpredictable and unexpected results. This is because there are multiple lines of dependent code which must be maintained in this model.
- **The SOA model as an incomplete solution:** The SOA model was designed to resolve problems caused by tight coupling and difficulties in code expansion found in the monolithic-architecture model. The majority of enterprises have shifted from monolithic-architecture to the SOA model in their IT architecture. The SOA mode divides a tightly coupled system into service-oriented, coarse-grained, loosely coupled, and stateless services. These services are connected to each other through the Enterprise Service Bus (ESB). However, this is not an ideal solution, because the ESB becomes the bottleneck of the system and prevents enterprise applications from developing towards cloudification that is also where the future lies.
- **The microservice model and cloudification:** The microservice model evolved from the SOA mode. It focuses on finer granularity, distributed deployment, and governance scalability of services. Each microservice is defined as a self-contained and independent application service free of external dependencies. Each microservice is capable of independently developing features, fixing bugs, and upgrading versions.

More and more enterprises recognize that microservice-based architecture will definitely be the preference for agile development of Cloud Native applications in the era of cloudification. Shifting to this new mode may increase complexity, for example, call chain and dependency management among multiple microservices can be a complicated issue. The PaaS platform is the inevitable solution to these new problems. It can provide unified services, microservice management, and runtime frameworks for the application layer, perfectly shielding complex resource distribution and deployment differences.

● New Silo Systems, a Result of Combining Fragmented Techniques in Implementing PaaS

Since enterprises have realized the importance of PaaS in recent years, departments within enterprises have accelerated the adoption and application of PaaS. However, a universally accepted technique for implementing PaaS has yet to reach the forefront, and different departments tend to use their own preferred techniques.

For example, R&D departments may emphasize acceleration of service innovation in order to reduce time spent in the development environment.

A unified PaaS aims to ensure that application development, application deployment, operations management, and organizational collaboration remain consistent with one another. >>

Therefore, they may prefer to choose techniques such as Cloud Foundry, which helps to create better development pipelines, support multiple languages, and enable multi-services access. On the other hand, O&M departments may prioritize the unification and standardization of IT resources and deployment required for all applications in order to optimize overall O&M efficiency, with an emphasis on cross-data center and global O&M efficiency. Therefore, those departments may prefer to use Kubernetes and Docker Compose/Swarm, which boast excellent open source architectures. In such cases, new silo systems are formed when new development platforms are constructed for the sake of more agile systems. This is counterproductive, as these differing development architectures and deployment modes will then hold back the progress of increased agility and high efficiency.

Unified PaaS: Driving the Transformation of Enterprise IT Application Development

Enterprise IT application development is a systematic issue, involving processes, methods, architecture, and organizations. In order to be effective, PaaS must be oriented toward the Cloud Native architecture of the future. Additionally, PaaS must be compatible with current enterprise SOA, be able to adapt with SOA, and be designated for applications.

To meet this need, a unified PaaS must be constructed, because it boosts the 'as-a-service' model and improves microservice development and management both technologically and architecturally. A unified PaaS can also unleash the full potential of development processes and organizational collaboration.

A unified PaaS aims to ensure that application development, application deployment, operations management, and organizational collaboration remain consistent with one another. This will help enterprises achieve agile development and service innovation while responding rapidly to their customers. The following section covers our proposal for creating three unified processes for a unified PaaS.

- Unified R&D Process Automation

Process automation is essential to a unified R&D process. Without automated tools, achieving true DevOps has proven to be an almost impossible task, as it is difficult to break barriers between development and O&M in a traditional R&D environment. The pipeline technology has been introduced during development in order to automate a series of R&D activities such as coding, compiling, testing, deployment, releasing, and upgrading. The pipeline acts as a bridge between development, testing, and O&M departments, driving efficient and effective inter-departmental collaboration. Though different enterprises use different development tools and conventions, the PaaS pipeline supports open ecosystem access and flexible process customization, allowing enterprises to tailor process automation to their needs.

- Unified Application Resource Orchestration and Scheduling

Resource orchestration and scheduling for deployment is mainly designed to achieve the efficient allocation and dynamic adjustment of inter-and intra-data center resources according to a Service Level Agreement (SLA). 'Efficient' is used here to describe quick scheduling and optimized resource utilization.

Application resources are diverse and complex, including hosts, networks, operating systems, databases, and middleware. Automated PaaS technologies will spur the automated application and scheduling of resources for development, deployment, and operations. This will achieve consistent, automated, and service-based Development, Test, Acceptance, and Production (DTAP).

In addition, self-service applications, deployments, and upgrades can be enabled within the PaaS environment at anytime, which can decrease the time developers spend on non-critical service activities by more than 40 percent, allowing them to focus on core business activities. PaaS also reduces service faults by managing the consistency of the running environment for development and production.

- Unified Microservice Management Frameworks for Large-Scale and Distributed Governance, Automated O&M, and Agile Operations

A traditional monolithic application can be transformed into a distributed application by dividing its services into microservices. For instance, how will microservices discover and communicate with each other? How will we track service call chains and locate problems? PaaS implements the unified microservice management framework on the distributed management layer, shielding complex functions such as mutual discovery, routing, call chain tracing, and disconnection. In this way, developers can focus on developing the service logic without the distraction of complex

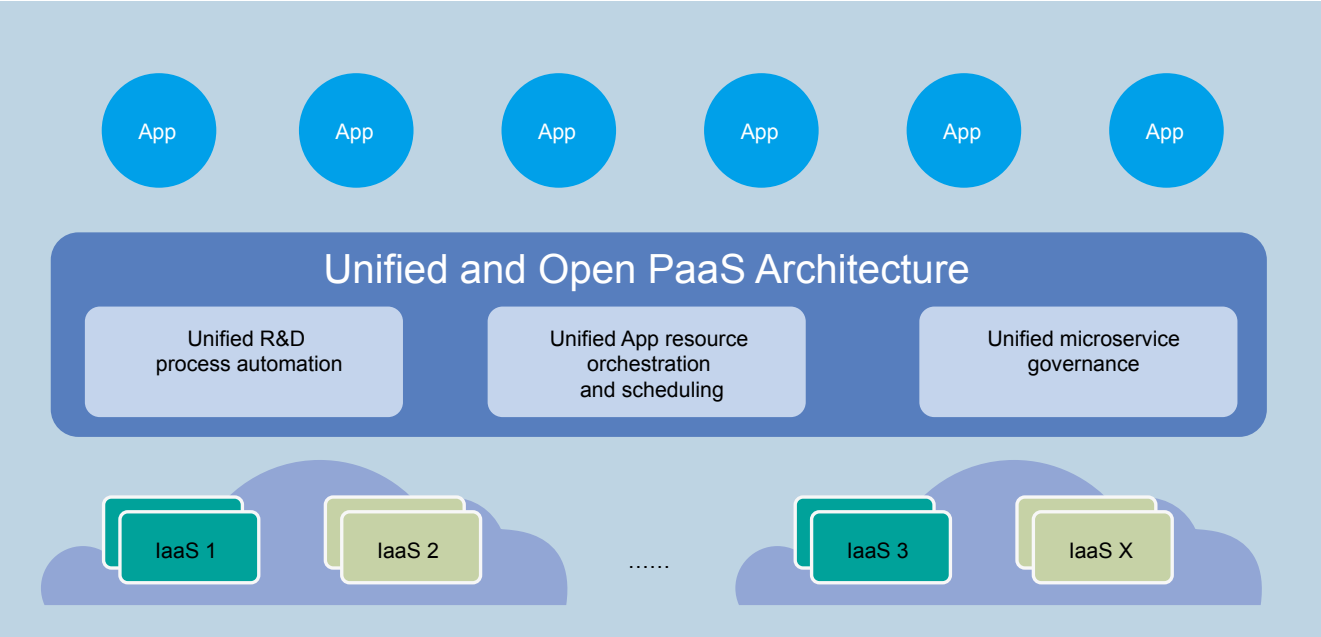


Figure 1: Unified and open PaaS architecture

> FusionStage is a universal PaaS platform providing development & deployment management, service operations management, and other public IT services. >>

management issues that can be caused by a distributed system. Each microservice team can develop and release services independently and rapidly. Though more agile than monolithic applications, distributed applications leave us with far more complex management issues.

Another key issue of PaaS microservice management framework is the management capability of existing SOA middleware in enterprises. Enterprises may have a large number of middleware services and it is impossible to transfer all of these services to the microservice architecture at the same time. Therefore, it is critical to build an appropriate middleware cloud to integrate these services to PaaS while shielding developers from implementation differences.

PaaS features the three unified processes, and supports the complete automation of the development, deployment, and operations of IT applications. This is a foundation for creating agile systems, which is also the ultimate goal of PaaS.

FusionStage PaaS for Agile Enterprise Transformation

Huawei, a leading global ICT solutions provider, operates in more than 170 countries in the enterprise, carrier, and consumer businesses. Huawei owns an IT system that provides technical support for customers, suppliers, partners, and Huawei employees around the globe. This complex system covers over 60 data centers, more than 1,000 applications, and tens of thousands of business processes. Each year, Huawei's IT system receives tens of thousands of new requirements and change requests, requiring an enormous investment in R&D.

In addition to being a customer-oriented business, the PaaS platform is also leading the way for Huawei's journey towards agile business operations and application development. With all of there in mind, Huawei has released the FusionStage PaaS. This platform is focused on unified automation of R&D processes, orchestration and scheduling of application resources, and management of microservices. It has been developed to implement automatic R&D, deployment, and operations, allowing it to support agile business operation.

With the FusionStage PaaS leading the way, Huawei is moving from IT 1.0 to IT 2.0, and will be implementing global data center deployment on the cloud. On this platform, applications in data centers located in eight regions around the globe can be deployed and upgraded at any time. Dozens of automatic deployments will happen every day, and thousands of releases can be automated each year. Application time to market will be reduced from weeks to days, leading to greater enterprise IT agility and efficiency.

FusionStage is a universal PaaS platform providing development & deployment management, service operations management, and other public IT services. With this platform, enterprises will be able to focus on developing their own services and applications, improving development efficiency, and implementing IT agility.

FusionStage PaaS will be deployed on the Huawei enterprise cloud and other public clouds, such as Open Telekom Cloud (OTC) for DT.

FusionStage revolutionizes how developers and enterprises work, transitioning them away from IT development and enabling them to zero-in on application development. Huawei is truly proud to announce the release of FusionStage and usher in an era of new, groundbreaking transformations. ▲

'On-Premises + Cloud:' **Achieving Cloud-Oriented Transformation of IT Applications**

By *Su Liqing*

Su Liqing

Smooth and steady cloud-oriented transformation of IT applications is obtainable by designing multi-layered and multi-leveled application policies, as well as adhering to the On-premises + Cloud strategy in the long term to leverage the advantages of both on-premises software packages and cloud-oriented applications.

As the most popular Information Technology (IT) buzzword in the past ten years, cloud computing has successfully realized sharing of IT resources and on-demand provisioning of services. Thanks to cloud computing, businesses are now able to innovate at lower costs and with enhanced agility. Cloud computing has not only changed the Internet industry; it has also affected and changed business and operating models, including the competitive landscapes across many enterprises and industries. Cloud computing has become the engine propelling the digital transformation of enterprises.

For enterprise applications, going cloud is an inevitable direction. This has become a consensus for various industries and enterprises. Along with the growing maturity of cloud computing, more and more enterprises are embracing the cloud. At Huawei Connect 2016, Huawei predicted that 'by 2025, all enterprises will be using cloud technologies and cloud models. In the past decade, only 20 percent of enterprise applications were running on the cloud, but by 2025, more than 85 percent of enterprise applications will be deployed on the cloud.' Most enterprises are exploring solutions that enable cloud-oriented applications, and are introducing Software-as-a-Service (SaaS) cloud applications and building and deploying IT applications based on cloud technologies and cloud architectures. In the future, enterprise applications will evolve towards the cloud at an increasingly faster pace, with the range of impacts being extended from non-critical business applications to production systems and critical business applications.

Top Challenge for Enterprises in Pursuit of Cloud-oriented Transformation

For more than 20 years, the processes and operating modes of enterprises were mostly implemented based on the Package Enabled Business Transformation (PEBT) model. Software packages were developed by integrating best practices of the industry and the needs of particular industries. The IT systems of most enterprises were constructed based on mature software packages such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Product Data Model (PDM). Software packages carried the key business transaction activities and customer data of enterprises, and became the backbone and important information assets for the IT applications of most enterprises. After long-term investment and construction, more than one hundred IT applications have been developed based on three major software packages, namely, EBS, Siebel, and Oracle Agile PLM. Software packages accounted for more than 80 percent of the applications running on the backbone network of Huawei.

However, with the rise of the Internet and mobile social networking, enterprise IT users require applications that operate in real-time and are easy to use. In this context, the disadvantages of traditional software packages in terms of response time, performance, and scalability were gradually exposed. Meanwhile, the coupled architectures of traditional

Applications that are based on traditional software packages have been unable to keep pace with and meet the requirements of users for flexibility and rapid innovations. >>

IT applications resulted in complicated relationships of integration between IT applications and difficulty in sharing functions. A minor change often required overhauling the entire system or architecture. Since software package-based application implementation and business innovation require a long period of time, applications that are based on traditional software packages have been unable to keep pace with and meet the requirements of users for flexibility and rapid innovations.

In addition, the industry still lacks new vendors who are able to provide mature and reliable cloud-oriented software packages that can be deployed on a large scale. The traditional mainstream software package providers are making very slow progress towards the cloud, and no major breakthroughs or advancements have been made as of yet. Therefore, companies cannot upgrade their internal on-premises software packages to cloud-oriented applications in a short period of time. Nor can they find completely new cloud plans to replace on-premises software packages.

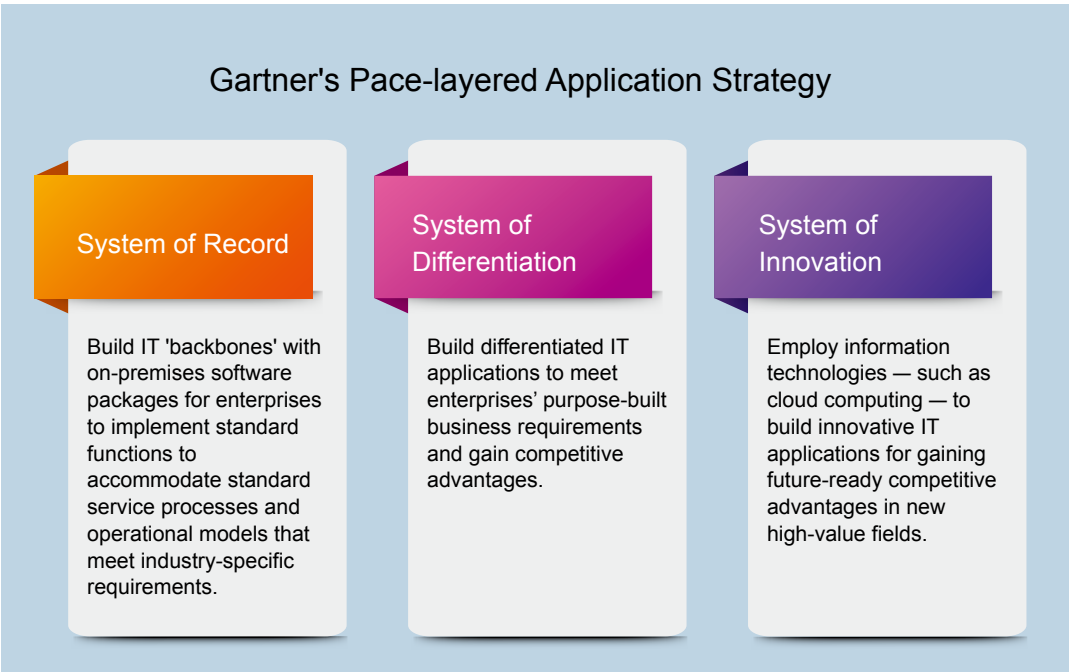
Other burdens of these companies include business processes and data that have been accumulated over the years and cost considerations. As a result, businesses not only lack the financial motivation to evolve their traditional IT applications to the cloud architecture, they are also unable to get rid of historical burdens and embark on an easy journey of cloud-oriented transformation.

Against this backdrop, achieving compatibility for and coordinating the development of both on-premises software packages and innovative cloud applications has become a long-term challenge to the IT departments of enterprises. While they aspire to embrace the cloud, enterprises must address the following three problems:

- Positioning of traditional on-premises software applications and innovative cloud-oriented applications in the IT architectures of enterprises
- Maximum exploration of the value of traditional on-premises software applications
- Quickly creating and deploying innovative cloud-oriented applications

On-premises + Cloud Strategy as a Basic Principle

On the one hand, enterprises need to persistently leverage the power of IT to drive innovation and improve their competitiveness. On the other hand, an important mission of enterprise IT is to ensure the stability and continuous opera-



The On-premises + Cloud strategy is a preferable choice that can protect existing investments, ensure business stability, and support smooth implementation of cloud-based enterprise IT applications. >>

tion of IT systems, and take into account business stability during innovation to prevent their core businesses from being interrupted.

Therefore, enterprise IT application cloudification and architectural upgrades will be a long and gradual process. For the time being, the On-premises + Cloud strategy is a preferable choice that can protect existing investments, ensure business stability, and support smooth implementation of cloud-based enterprise IT applications. During the process of application cloudification, on-premises software packages will remain as the backbone of IT applications and play an important role. On-premises software packages and cloud-based applications will coexist for a long time, forming a hybrid IT architecture that features On-premises + Cloud.

Five Ways to Compatibility and Coordinated Development

● Formulating Multi-layered and Multi-leveled IT Application Policies

In 2011, Gartner released the 'Pace-Layered Application Strategy,' which divides IT applications into three layers based on the degree of standardization of supporting facilities. The three layers are top, middle, and bottom, as shown in the following figure:

- The bottom layer is a System of Record that provides back-end backbone applications. This layer uses primarily on-premises software packages to construct the IT 'backbone' of an enterprise, supports standard business processes and modes of operation using standard features, and meets particular industry requirements, such as in the case of an ERP financial module integrating industry-specific accounting standards.
- The middle layer is a System of Differentiation that is intended to meet the special needs of enterprises and help them build up differentiated competitiveness by deploying customized IT applications based on software packages.
- The top layer is a System of Innovation oriented to customer access or new and high-value areas. To meet the requirements for real-time service experiences and ease of use, this layer uses cloud computing and other IT technologies to build innovative IT applications that enable enterprises to possess future-proof competitive advantages.

This multi-layered and multi-leveled strategy provides a good reference for the evolution of IT application architectures. The back-end uses primarily on-premises software packages to construct a backbone that supports core processes and data such as order processing, supply, and delivery. Other businesses, such as sales, customer service, and manufacturing can deploy differentiated applications and innovative cloud applications to build up differentiated competitiveness. In the future, back-end applications will remain basically stable, and differentiated and innovative cloud applications will account for an increasingly higher

percentage of the internal IT application portfolio of enterprises.

- Exploring the True Value of On-premises Software Packages and Delivering Service-oriented Functions

On the one hand, the advantages of on-premises software packages in terms of business and data logic must be best utilized. For the internal IT applications of enterprises, software packages are meant to constitute the back-end, that is, the System of Record, which uses standardized software packages to implement the transaction model and the main data model, thereby ensuring the stability of the business flows of enterprises.

On the other hand, efforts must be taken to bypass the disadvantages of on-premises software packages that are being used. In typical cases, the IT system of an enterprise can have several hundred applications. To avoid duplicated development of the same functions and applications and to share the functions of software packages, the IT department of the enterprise can decouple the architectures of applications and introduce the Service Oriented Architecture (SOA). This approach allows the functions of a software package to be exposed and encapsulated into individual services. After encapsulation and service-oriented processing, software packages can be completely open to business services, providing extensive, diversified, and shared business functions to facilitate the construction of a System of Differentiation and a System of Innovation for the front-end, thereby avoiding duplicated development efforts.

> A powerful middle platform between front-end innovative applications and back-end software packages will be responsible for managing and utilizing services to achieve the purposes of rapid innovation and interworking. >>

- Building a Middle Platform to Support Collaboration Between On-premises Software Packages and Cloud-based Applications

With the emergence of service-oriented functions of software packages and increasing numbers of cloud-based innovative applications, enterprises will encounter some new problems. For example, how do we effectively share and use applications that are scattered across different IT systems? How can we quickly achieve interworking between innovative front-end applications and back-end software packages? To achieve these goals, it is necessary to construct and introduce a powerful middle platform between front-end innovative applications and back-end software packages. This middle platform will be responsible for managing and utilizing services to achieve the purposes of rapid innovation and interworking between front-end innovative applications and back-end software packages.

In another example, we constructed an 'order processing middle platform' geared to support the online sales of Huawei mobile phones. This middle platform provides basic capabilities and shares both business and IT services. For the upper layer, the middle platform supports quick development of diversified innovative applications oriented to various scenarios, including To Business (2B) and To Customer (2C). For the lower layer, the middle platform supports standardized interworking with back-end software packages. In the past, if you wanted to open a shop on a third-party website, it generally took three to six months to achieve inter-

working with back-end applications. Now, through the construction of a middle platform that realizes standardized interworking between back-end software packages and third-party applications, the amount of time needed to open an online shop is reduced to one or two weeks. In addition, the middle platform can also help consolidate business rules. For example, thanks to automated processing of routine operations such as purchase order handling and approval, the amount of time that is needed for a purchase order to be processed decreases from two days to merely several seconds, thereby realizing automated business processes and rapid transaction handling.

The middle platform is an important part of the enterprise IT system, and contributes to both the agility of front-end services and stability of the back-end. Future IT architectures will feature a lightweight front-end, powerful middle platform, and stable back-end. The front-end is intended to achieve agile and rapid innovation oriented to businesses and business objects, thereby improving business efficiency and the user experience. The middle platform shares capabilities and business and IT services. It consolidates transaction rules and realizes automated business processes and rapid transaction handling. The back-end uses software packages as its backbone, and carries standardized business models and primary data model to ensure business stability.

- Evolving Applications to the Microservice Architecture to Lower the Difficulty in Achieving Cloud-oriented Transformation

In the past, enterprise IT departments had to manage huge numbers of applications that were closely coupled in architectures. This situation was unfavorable to achieving rapid construction and continuous deployment of applications, causing tremendous difficulties to cloud-oriented transformation. In recent years, Amazon, Netflix, and other Internet companies adopted the microservice architecture to resolve the issue of application complexity. What these companies developed are no longer giant monolith applications. Instead, a single giant monolith application was split into multiple smaller microservices, each of which is generally intended to complete a specific function, such as purchase order management or customer management. Every application function is implemented by a corresponding microservice, and multiple interrelated microservices implement the overall function of the application.

One microservice can be developed, deployed, and maintained separately as an application, without the need to consider the impact that may be generated due to the development of other services. Thanks to the microservice architecture, continuous construction and deployment of applications based cloud technologies and architectures become possible, greatly reducing the difficulty in achieving cloud-oriented transformation for applications.

- Supporting Cloud-oriented Applications with IaaS and PaaS

Cloud-oriented transformation of applications requires support from powerful technology platforms, and cloud-oriented applications must be constructed and deployed based on Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) that are particularly geared towards the cloud. A cloud-oriented and service-oriented IaaS layer can reduce the amount of time needed to obtain calculation, storage, and network resources, and meet the requirements of applications for elastic and scalable IaaS resources. By constructing a unified cloud- and service-oriented PaaS platform, an enterprise is able to resolve a number of issues, including duplicated development of common functions of applications, middleware, and databases for multiple applications, and slow application deployment and difficulty in performance scale-up. The IT department of an enterprise is expected to provide flexible and scalable IaaS and PaaS services that would allow business departments to focus on business innovations without being concerned about the acquisition of bottom-layer resources.

The cloud-oriented transformation of enterprise IT applications is a long process that cannot be achieved overnight. The core issues are the evolution and coordinated development of on-premises software packages and cloud applications. Smooth and steady cloud-oriented transformation of IT applications is obtainable by designing multi-layered and multi-leveled application policies, as well as adhering to the On-premises + Cloud strategy in the long term to leverage the advantages of both on-premises software packages and cloud-oriented applications. ▲

The IT department of an enterprise is expected to provide flexible and scalable IaaS and PaaS services that would allow business departments to focus on business innovations without being concerned about the acquisition of bottom-layer resources. >>

On-Demand SDN Architecture across **Private and Public Clouds**

By *Huang He*

With the development and gradual maturation of public clouds, more and more enterprises are starting to use public cloud services, at first to carry non-key services or disaster recovery services and, eventually, to carry key applications. Of course, development does not happen overnight, and, in addition, some applications will ultimately still use private clouds. Therefore, in the long term, hybrid clouds are the fundamental form of the enterprise IT architecture. It is well known that the biggest advantage of cloud services is flexible IT resource sharing, and so networks across private and public clouds must also be flexible for effective hybrid cloud development support.

Huang He

Cloud service development is a long-term process. Hybrid clouds will be the fundamental and long-term architecture for IT enterprises. Hybrid clouds require on-demand networks across private and public clouds to achieve the desired agility, and, for this, a network that features the SDN architecture is undoubtedly the best choice.

On-demand Networks are a Fundamental Requirement of Cloud Service Development

Hybrid clouds provide enterprise applications with the benefits from both public and private clouds, but they also face a variety of challenges regarding inter-cloud network interoperation, network latency, multi-vendor heterogeneity, and network resource scalability necessitated by flexible cloud resource scalability.

- **Networks require higher performance imposed by scale and demand:** As cloud application development continues apace, the number of enterprise users, the scale of DCs, and the amount of cloud service data and traffic, as well as meeting user needs are all continually increasing. Not only is there a need to deal with the issues of mass NE management and dynamic scaling, but also increasingly higher requirements are put forward by a large number of tenants regarding network capacity, service deployment time, and convergence performance.
- **Cross-DC unified resource orchestration and VPN deployment between DCs:** Interconnections among multiple DCs often require complex external networks spread across long distances. In addition, support for the unified orchestration of private and public cloud services is required so applications can be automatically migrated within public and private clouds based on service requirements.
- **Multi-vendor interoperability:** Hybrid cloud infrastructure is, by necessity, multi-vendor heterogeneous. Achieving seamless integration of products from different vendors, as well as unified management and O&M, is a problem that all hybrid cloud solutions must tackle.
- **E2E streamlined DC, campus, and WAN (IP/optical) networks:** As enterprises deploy data and services on the cloud, the distance between users and their data objectively increases. As a result, network borders must be broken in order to achieve the unified management and scheduling of network resources. A unified network resource pool can be achieved through the synergy of IP and optical layers.
- **Clouds require application-oriented, on-demand, auto-scaling, and cloud-adaptive networks:** Application-oriented networks enable IT administrators to define network requirements using service-based language from service perspectives, as well as implement automated application-based network resource scheduling to allow their networks to support on-demand intelligent cloud connection.

SDN Architecture: Best Choice across Private and Public Clouds

SDN redefines network capabilities from a software perspective, solving problems that many traditional networks simply cannot. SDN technology enables networks to move with the cloud — allowing dynamic changes in real time based on application and service requirements. SDN also improves network O&M efficiency — reducing O&M costs by 40 percent through automated network management and fault rectification. In addition, SDN implements network traffic steering in a centralized control manner, significantly improving network utilization and fault tolerance. For example, with the help of the Huawei Agile Controller, 21Vianet has achieved an increase from 50 to 80 percent in link utilization between DCs.

Through its open network capabilities, SDN allows enterprise users to configure their networks based on service requirements, as well as implement Network-as-a-Service (NaaS) and network and bandwidth on demand. This is the most important part of a hybrid cloud's network architecture. In addition, to better meet hybrid cloud requirements, SDN networks provide the following functions and features.

● Flexibility and Scalability

The hybrid cloud network is scalable enough to handle sharp increases in cloud tenants and services. When the number of devices in a DC, on a WAN, or on a campus network increases, the SDN controller is still able to maintain unified control of the network. Two key technologies support SDN's network control flexibility: controller cluster and controller federation.

Based on domain-specific control, the SDN solution can implement E2E control in any scenario and provides network-wide resources on demand, automated deployment, and intelligent traffic control. >>

• **Controller cluster:** Limited by the server's processing capabilities, single-node controller networks can control a maximum of thousands of hosts. However, using a cluster consisting of multiple controller nodes arranged in a distributed architecture greatly improves network management capabilities. In this way, controller clusters are able to support mass device management and transaction consistency on large-scale hybrid cloud networks.

• **Controller federation:** In cross-DC, cross-region hybrid cloud scenarios, a single controller cluster managing multiple DCs will result in problems such as limited scale and poor reliability, which can easily result in 'split-brain' issues. The SDN controller federation architecture can completely solve this problem, providing support for cross-cloud application data migration and cloud service expansion. The controller federation architecture provides both scalability and processing performance. Domain controllers are responsible for local control-plane processing, specifically providing low-latency assurance. A 'super controller' is responsible for the processing coordination of multiple domain controllers in order to implement network expansion.

● E2E Control in any Scenario

Hybrid cloud networks consist of cloud access networks and interconnected public and private cloud networks that span multiple networks, including campus, WAN (IP/MPLS and optical transport), and DC networks. Based on domain-specific control, the SDN solution can implement End-to-End (E2E) control in any scenario and provides network-wide resources on demand, automated deployment, and intelligent traffic control. To support more complex intelligent applications, coordination between domain controllers through orchestrators or super controllers is required. Due to the differing characteristics of each application scenario, the SDN controller architecture must have a flexible framework.

● SDN Northbound Openness

Northbound openness is one of the most important features of the SDN architecture. Northbound openness gives SDN networks incomparable advantages over traditional networks, including:

• **Network programmability:** This transforms network resources and capabilities, making services open to users, and so accelerating service innovation.

• **System integration:** The controller can be conveniently integrated with the orchestrator, cloud management platform, and BSS/OSS through open northbound interfaces.

• **Evolvable platform:** Apps can be decoupled from the controller platform, achieving backward compatibility, without platform replacement or large-scale reconstruction.

To achieve northbound openness, the controller needs to provide not only network models based on defined open

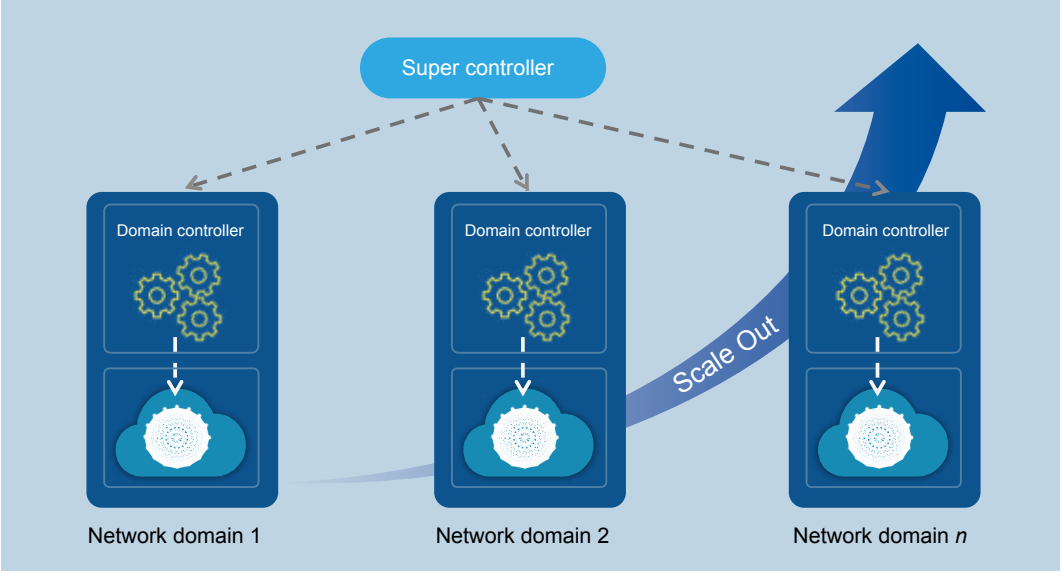


Figure 1: Federated clusters for network flexibility

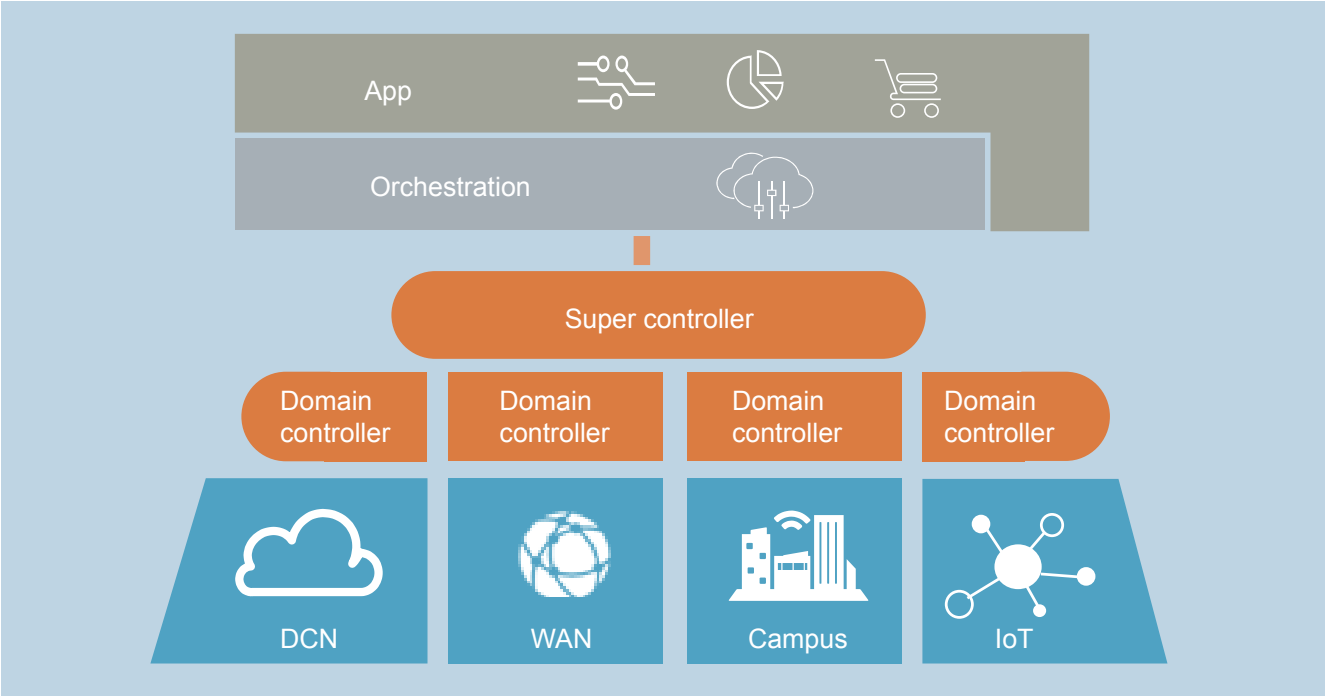


Figure 2: On-demand deployment and intelligent traffic control

standards but also those based on the de facto standards of open-source platforms.

- Southbound Multi-vendor Heterogeneity

To achieve network programmability, the SDN controller uses southbound network control technology to manage and control the entire network device layer, including topology discovery, status collection, policy management, network configuration, path optimization, and forwarding entry delivery. The network structure is complicated and involves a wide variety of equipment vendors, and the goal of carriers and enterprises is to avoid vendor lockout. SDN controller southbound interfaces must:

- Support multi-vendor heterogeneity
- Mask the differences between interfaces on devices from different vendors
- Abstract physical devices to facilitate the management of pooled logical resources
- Support interconnection with third-party VAS devices to provide value-added services

To support multi-vendor heterogeneity, SDN controllers need to provide a southbound-driven mechanism and adopt plug-in technology so third-party vendors can flexibly develop customized plug-ins that support dynamic loading.

- High Network Reliability

SDN networks are a restructuring of traditional networks and involve a moving away from distributed control to centralized control. However, one of the downsides to centralized control is that controllers as the centralized control points may experience faults, and links between controllers and their respective managed networks may also encounter faults. As networks are the basic infrastructure of telecommunication systems, network disruptions and forwarding failures are of zero tolerance.

> SDN controllers provide the following capabilities: E2E agile interconnection, intelligent on-demand bandwidth optimization, and intelligent network O&M. >>

Solving the issue of SDN reliability is a progressive process involving the following steps. First, controller products must come with their own multi-layered, reliability-ensuring systems. This should include the use of distributed systems to achieve cluster reliability and geographical redundancy, the use of load balancing to increase northbound reliability, and the use of southbound transaction and reconciliation systems to achieve data consistency between the controller and forwarding plane.

Second, the reliability of the connection channel between the controller and forwarding plane must also be ensured. For this purpose, redundant links are often used in order to ensure uninterrupted access between the network and controller.

- SDN Network Intelligentization

Network intelligentization is the key difference between SDN networks and traditional networks. As a network's 'brain,' SDN controllers are the key components in the process of network intelligentization and provide the following capabilities: E2E agile interconnection from a global network perspective and intelligent on-demand bandwidth optimization, and intelligent network O&M with rapid troubleshooting and self-healing capabilities as a result of network resource pooling.

The SDN controller provides network optimization solutions that are flexible, efficient, intelligent, and in real time. By having a global network view, it can provide E2E

application-based optimization for enterprise branches, WANs, and DCN networks. To perform intelligent network control, the SDN controller must be able to support network-wide topology discovery and service status (bandwidth, latency, jitter, packet loss rate, etc.) monitoring. Based on real-time network and service data, and user-defined network service requirements, the SDN controller uses global path optimization algorithms to implement network traffic scheduling and achieve network service perception and Bandwidth on Demand (BOD).

SDN approaches the task of intelligent network O&M from a usability perspective, utilizing a diverse set of fault-detection methods, Big Data analysis platforms, and intelligent fault-decision-tree analysis to provide an efficient, intelligent, rapid, and self-healing O&M framework. This frees O&M personnel from their previously tedious workload and creates a framework for the automation of O&M-related tasks.

SDN Solution Deployment Phases and Commercial Practice

Total network transformation cannot happen overnight, and SDN deployment plans must adopt a flexible evolution pathway. This must take place while maintaining a focus on clouds as they extend from individual network scenarios to cross-network scenarios and then to E2E network scenarios, eventually achieving E2E NaaS. Deployment should be divided into three phases — 'placing points,' 'connecting points to lines,' and 'forming a plane from lines' — in order to facilitate hybrid cloud construction with a network-wide SDN solution.

> SDN deployment plans should be divided into three phases — 'placing points,' 'connecting points to lines,' and 'forming a plane from lines' — in order to facilitate hybrid cloud construction with a network-wide SDN solution. >>

- Phase I: Placing Points — Deployment of Domain-specific SDN Solutions

Technological development always requires you to start with the basics and gradually increase complexity over time. Any carrier, enterprise, or equipment supplier wishing to take part in SDN development must begin from a single domain, which means a single DC, WAN, or campus network. Dedicated enterprise lines to cloud servers also begin with overlay solutions directly creating site-to-site and site-to-cloud overlay tunnels in order to open dedicated lines rapidly and avoid the complexities associated with cross-domain WAN and cross-vendor and cross-technology interconnections.

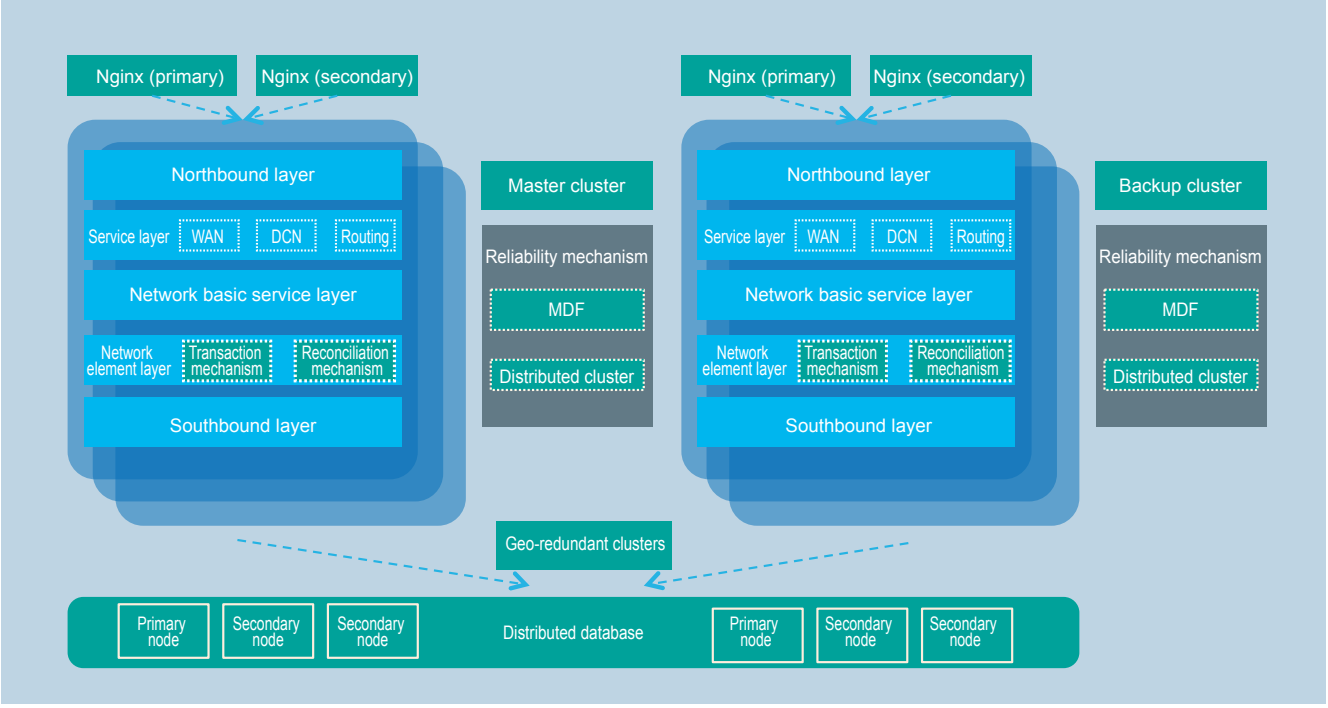


Figure 3: SDN architecture with Nginx server

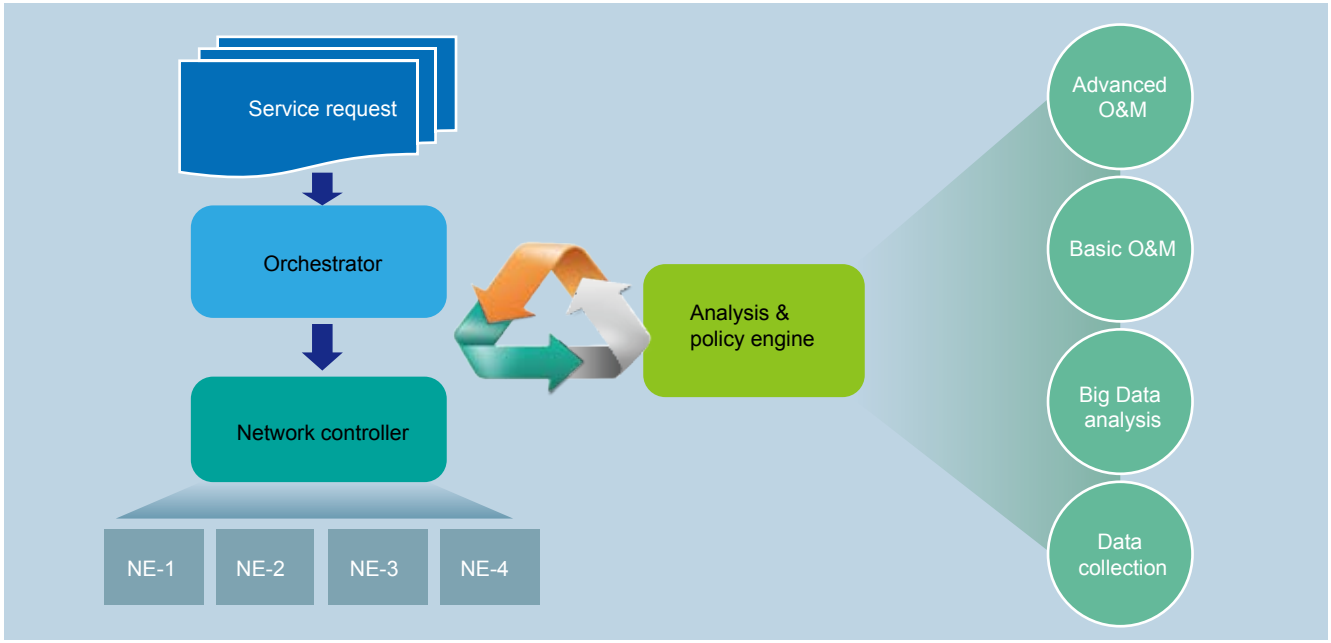


Figure 4: SDN O&M intelligence functions

● Phase II: Connecting Points to Lines — Cross-Scenario Unity, Point Infiltration, and Application Expansion

After the successful implementation of the domain-specific solutions, carriers will gradually stitch together the deployment of cross-domain networks, extending the application range of SDN. This includes the following combinations:

- DCN and DCI orchestration, achieved by integrating the DCN and WAN to implement cloud-network synergy, which is the dynamic scheduling of network resources based on cloud application requirements (bandwidth, latency, etc.)
- Multi-domain control, achieved by coordinating the backbone, metro, and campus networks into one network to implement E2E automation and cross-domain traffic optimization
- IP + optical synergy, achieved by managing optical, electrical, Ethernet, and IP resources as a unified resource pool to improve network resource utilization

● Phase III: Forming a Plane from Lines — Implementing E2E NaaS with Cloud-Pipe-Device Synergy

With cloud-pipe-device synergy, the evolution of the bearer network from overlay to underlay, and the management of the entire network as a resource pool, network on demand for cloud connect will finally be achieved. Networks will be able to adapt dynamically to the demand of cloud services, providing E2E QoS and SLA, and providing high-quality connections for 4K video, video conferencing, the IoT, 5G, and financial services.

SDN has already been proposed for several years, during which Huawei has done a lot of exploration work, especially in cloud service scenarios where many commercial practices have been completed. Such cases include Deutsche Telekom (DT) and China Telecom.

In March 2016, DT and Huawei jointly announced the official unveiling of an open telecom cloud. DT chose Huawei to provide hardware and software solutions for its telecom cloud. When customers migrate their IT services to the cloud, they can perfectly balance prices, services, and quality. The SDN-based hybrid cloud deployment solution will further help customers carry out their hybrid cloud strategy.

In 2016, Huawei assisted China Telecom in constructing the IDC backbone bearer network by providing an SDN DCI solution that matched the innovative E-Surfing cloud-network synergy mode. The Huawei SDN DCI solution provided a high-performance dedicated cloud bearer network with ultra-wide pipes, ultra-low latency, network on demand for cloud connect, and cloud-based network resource sharing.

The development of cloud services is a long-term process, and the hybrid cloud will be the fundamental and long-term form of the enterprise IT infrastructure. The hybrid cloud requires 'on-demand networks across private and public clouds' to achieve agility, and SDN networks are undoubtedly the best choice. Huawei's leading, open, scalable, and highly reliable SDN controller and network equipment solutions meet the development needs of the hybrid cloud, enabling customers to build an agile IT system to advance the development of their business and enjoy the true value of clouds.▲

Huawei's SDN controller and network equipment solutions enable customers to build an agile IT system to advance the development of their business and enjoy the true value of clouds. >>

Developing a Scale-Out Data Center Network with the Cloud

By *Yan Qinghua and Zhu Guangping*

Living in an information society, we are producing an exponentially growing volume of information year by year. As storage, processing, and analysis of data primarily take place in data centers, new demands and challenges are brought to the data center network. At the moment, we must explore ways of dealing with these demands and challenges.

New Demands and Challenges to Cloud Data Center Network

As we all know, the core concepts of cloud computing are based on pooled hardware resources, fully distributed software, and fully automated operations. The basic need of this new distributed computing and storage architecture is to access data across multiple compute nodes. As a result, east-west traffic within the data center is far larger than north-south traffic between the data center and users and, in some scenarios, such as searching, east-west traffic can be 40 times more than north-south traffic. Since non-blocking networks are essential for implementing cloud computing, the current converged Clos data center networking architecture is confronted with new challenges.

● Capacity Demand for Petabit-level Non-blocking Switch

A typical cloud data center consists of 50,000 to 100,000 servers. These servers can be either located within one large data center base or distributed in multiple server rooms within a radius of 200 kilometers. Three to four thousand servers can constitute a Point-of-Delivery (PoD) cluster in which a strict non-blocking network is implemented. Between clusters, the non-blocking network is implemented to the maximum possible extent so as to enable computing and sharing on a larger scale. In this scenario, the network demand for switching capacity is extremely high. With four 10G ports on each server to achieve a network capacity of 2 to 4 petabits, the demand for network capacity of the cloud data center will reach the petabit level (1 Pbit = 1,000 Tbits), even based on a convergence ratio of 1:4 between clusters.

Yan Qinghua

Zhu Guangping

Scale-out networking architecture can be built in a MESH^2-based data center network by adopting the concepts and ideas of cloud computing and using optical network technologies. It is poised to become the focus of future development of cloud data center networks.

For a conventional networking architecture based on device convergence, the maximum capacity of its core switch is about 50 Tbit/s. If the networking architecture remains unchanged to meet future demand, the capacity of the core switch has to reach over 200 Tbit/s; however, it is very difficult to increase the SerDes speed and the unit capacity using technologies that are based on electrical interconnections. Moreover, the impact of a Single Point of Failure (SPoF) will become greater, resulting in high costs that discredit SerDes as a sustainable approach.

- Network Devices Require High Power Density

Power consumption is also a huge challenge to data centers. There are many big power consumers among the facilities of a data center that have long been dubbed 'power killers.' More importantly, a uniform density of energy must be guaranteed because uneven density of energy can greatly affect the power system, cooling system, data center space, and data center security.

Because of its huge capacity, a typical core switch has the power of nearly 30 kilowatts. The power supply capacity of a single rack in an old server room, however, is merely four to five kilowatts, while that in a new server room ranges from eight to 12 kilowatts. If the power consumption of a single device is too large, adequate space must be kept all around it to ensure its power supply. Moreover, since the working conditions of the cooling system must be perfectly ensured, it will be difficult to increase the spatial distribution density of the entire server room, and great challenges will be brought to the cooling for power supply. With the increasing size of the network, power consumption and cooling become more and more pressing issues that call for more efficient resolutions.

- Massive Fiber Connections: A Bottleneck for Data Center Operation, Maintenance, and Scalability

For the connection of a conventional Layer-3 network device, traffic between groups of the Top-of-Rack (ToR) switches should be ultimately forwarded by the core switch. In other words, the optical fibers should be converged in the core server room. As a result, a 'fiber wall' problem is caused in which the dense fibers resemble a wall, complicating Operations and Maintenance (O&M) of the data center.

The number of fibers can be reduced using large-capacity ports, such as 40 Gigabit Ethernet (GE) or 100 GE ports. However, given the cost of the optical module, the multi-mode parallel optical module of 4 x 10 GB or 10 x 10 GB is usually adopted because a 40 GE port requires four pairs of optical fibers while a 100 GE port requires 10 pairs. This means that the number of fibers is not reduced, and the great challenges to O&M remain the same. Meanwhile, in the design of the ToR in a server room, the general specifications support about 2,000 bundles of fibers. For this reason, the number of connected fibers in the core room further limits the capacity of non-blocking switching in the entire network to a maximum of nearly 200 Tbit/s (2,000 x 100 GE).

Therefore, with the development of cloud computing, the cloud data center is becoming larger and larger in size, with growing east-west traffic. The data center network will face new demands, especially with the capacity demand for petabit-level non-blocking; however, the conventional networking architectures are confronted with a series of difficult problems in capacity, power supply, power consumption, scalability, and O&M, all of which can only be resolved with a new architecture.

Building Scale-out Data Center Networks

Besides the scale-up approach that makes larger single devices, is there an alternative solution using the approach of scale-out that can resolve the capacity problem? Our answer is yes, and we have proposed the MESH^2 networking architecture.

- MESH^2 Networking Architecture: Building Scale-out Data Center Networks Using an Optical and Distributed Approach

MESH^2 networking architecture, also known as two-level Mesh networking architecture, is a distributed network topology that adopts the scale-out approach of cloud computing. The idea of cloud computing is to build super-large capacity of storage and computing by using 'small particles

The cloud data center is becoming larger and larger in size. The data center network will face new demands, including capacity, power supply, power consumption, scalability, and O&M, all of which can only be resolved with a new architecture. >>

of hardware + large-scale distributed software.' With this approach, the cost of the system can be lowered by replacing the reliability of a single device with that of a distributed system. MESH^2 networking architecture results from this idea, with its overall logical structure (Figure 1).

The MESH^2 networking architecture has a number of key features. The first feature is super-flat, as there is only one layer of ToR switches in the entire network, directly deployed in each server cabinet. By changing the multi-level convergent structure of the data center network into a one-layer physical network structure, the entire network is connected by small switches of the same specification and configuration. Each switch is connected by both intra-group MESH and inter-group MESH, eliminating the need for the large-capacity convergent and core switches in a conventional architecture.

The ports of each ToR switch are divided into three groups. The first group is the local ports that connect to the server. The second group is the intra-group connection ports that connect to other ToR switchers within the same PoD, forming an intra-group one-level MESH connection. The third group is the inter-group connection ports that connect ToR switches between different PoDs in the same inter-group plane, forming an inter-group two-level MESH connection. A standard two-level MESH network consists of N x N ToR nodes: There are N PODs, each of which has N ToR nodes.

The second feature is that, when the optical network enters the data center, Wavelength-Division Multiplexing (WDM) and passive optical device Cyclic Array Waveguide Grating (CAWG) are used to implement the MESH interconnection. Both the intra- and inter-group MESH connections require direct connection of the fiber to the associated nodes. If the network size is very large, say, one with 48 x 48 nodes, the number of fibers connected to the network can be enormous, as hundreds of thousands of pairs of fibers may be required, and the node direction of each connected fiber varies. To resolve the MESH connection problem of the optical fiber, WDM interfaces and CAWG are introduced. WDM interfaces can be either built inside switches or deployed independently. After multiplexing, the N transmit ports of ToR switches are connected to the input fiber of CAWG. This optical device not only converts logical MESH connections in switches to a physical star connection but also resolves the problem of massive fiber connections that affect a large-scale data center network.

The third feature is that the distributed forwarding of MESH^2 network enables non-blocking switching and smart route scheduling, thereby improving the network throughput. The MESH network is physically a one-layer network, but it is still a three-layered Clos network in the forwarding model. It is distributed, that is, the ToR switches perform all functions of the switches at the three layers: ToR, convergence, and core. In this way, the capabilities of the convergence and core switches are distributed to each ToR switch, eliminating the central point and bottleneck of the system. Moreover, unlike the conventional Clos architecture, the hop count of traffic forwarded in the data center can be reduced by a smart UCMP path route-scheduling algorithm in a MESH network, due to the presence of the direct path. This significantly reduces delay and improves the forwarding efficiency of the MESH network.

- Merits of Scale-out Architecture: Super-large Capacity, Decentralization, Easy Maintenance, and High System Reliability

The new architecture actually reallocates the switching capability of aggregation and core switches in the traditional three-layer Clos network to ToRs in the MESH^2 network, which breaks through the bottlenecks of traditional networks. Its values are described as:

First, a fully distributed flat architecture breaks the limit on capacity by allowing the construction of a network with a super-large capacity. A two-level MESH^2 network can be used to set up a non-blocking data center network with Pbit/s-level switching capacity — where 1 Pbit/s has the capacity to support 50,000 servers with dual 10 Gbit/s ports. The capacity demand for each ToR is 5 x 48 x 10 Gbit/s = 2.4 Tbit/s, which can be provided by two hundred and forty 10 Gbit/s ports, or forty-eight 10 Gbit/s ports (connecting to the server) and ninety-six 25 Gbit/s ports (connecting between the ToRs). It is easy for the ToRs to deliver such a capability. In contrast, if a conventional Clos network is adopted, the core switches will need a switching capacity of more than 200 Tbit/s, which will be extremely challenging.

Second, the introduction of a decentralized architecture and optical technology eliminates the engineering limits on power consumption, cooling, wiring, and maintenance. The

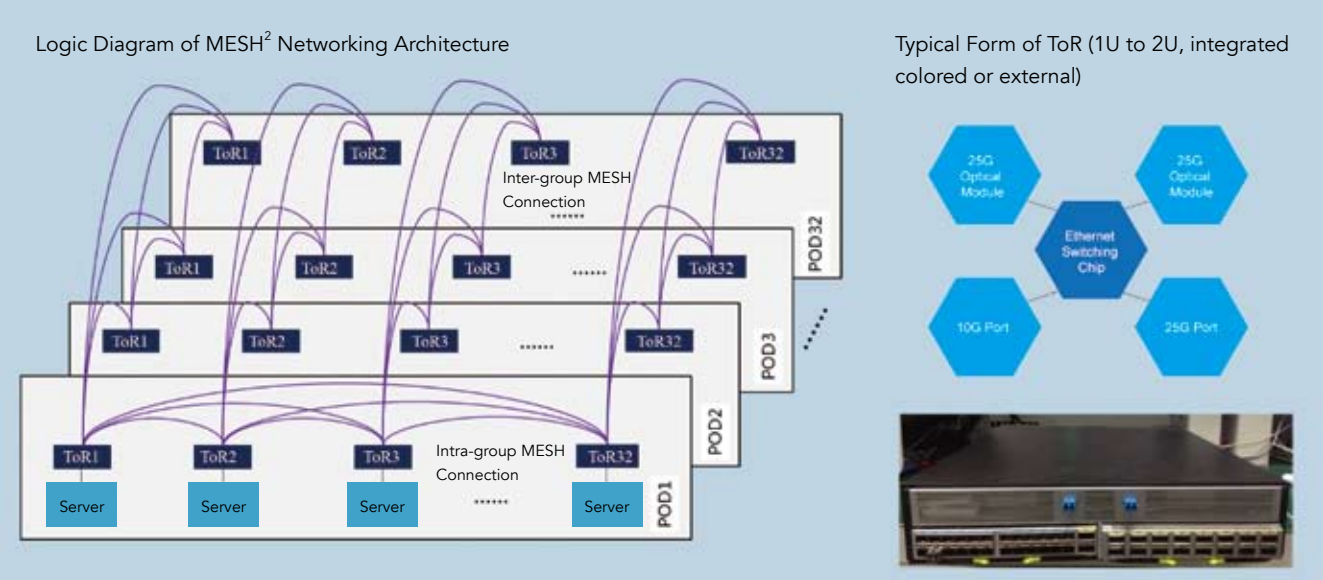


Figure 1: MESH² networking architecture with its overall logical structure

new architecture removes the need for large devices, such as the core and convergence switches, leaving only the ToR switches, similar to a rack server. As a result, the system gets rid of the big power consumers, making power supply, cooling, and security no longer a problem for data centers. At the same time, the introduction of WDM and CAWG decreases the number of fiber connections in the entire network by several dozen times and evenly distributes the connections among server room modules, greatly simplifying the issues of cabling and O&M, and significantly reducing the costs of open O&M.

Third, replacing the reliability an individual large device with that of a distributed system eliminates the risk of SPoFs. In a conventional data center, with the increase in switching capacity, the roles of the nodes at the convergence and core layers become more prominent. Especially in a converged topology, the failure of a core switch can produce tremendous impacts on the traffic switching of the entire network, so the staff must be particularly careful during the maintenance of convergence and core nodes. However, in the new architecture, there is only one layer of physical network nodes (ToRs) in the entire network. Due to the large number of ToRs, the failure of a single node only affects the traffic switching in the respective cabinet server, accounting for only a few thousandths of the entire network. This completely rules out the possibility of a node failure leading to a large-scale network breakdown and greatly enhances the reliability of the network.

Problems and Prospects of the Scale-out Network

Nevertheless, the scale-out network has two shortcomings. One is that CAWG only provides wavelength cross-connection in a fixed direction, restraining flexible networking and seamless scaling. The other is that the bandwidths of the interconnection ports between ToRs are the same, allowing only an overall upgrade instead of a flexible upgrade. Although these problems can be avoided or optimized by engineering methods, project deployment modes, or practical applications, they cannot be completely resolved and can only be addressed through further innovation, such as flexible optical cross-connection technologies and optical ports with variable bandwidths. The progress of these optical technologies will also become the focus of the future development of data center networks, resulting in the construction of the data center network on the basis of optical technologies and optical networks.

“As it resolves the engineering problems in power consumption, cooling, cabling, and maintenance, and reduces the risk of SPoFs, scale-out networking architecture is poised to become the focus of future development of cloud data center networks. >>”

With the development of cloud computing and services, the explosive growth of information and changes in the data traffic model are bringing unprecedented demands and challenges to the data center network. In this regard, it is necessary to adopt new thinking, designs, and technical architectures to reshape the future of the data center network.

Scale-out networking architecture can be built in a MESH²-based data center network by adopting the concepts and ideas of cloud computing and using the technologies of optical network. It can resolve the problems that are difficult to overcome in the conventional Clos networking architecture and build super-large petabit-level capacity and achieve higher network efficiency through a fully integrated one-layer networking architecture and smart route scheduling algorithms. As it resolves the engineering problems in power consumption, cooling, cabling, and maintenance, and reduces the risk of SPFs, scale-out networking architecture is poised to become the focus of future development of cloud data center networks.▲

Intelligent O&M in Future Cloud Data Centers

By *Ma Li*

In the cloud computing era, IT system builds are becoming an increasingly vital link to achieving development agendas. Business systems and the infrastructure supporting those systems are a prime point of concern for many enterprises. Operations and Maintenance (O&M) systems are the 'heroes behind the scenes' that keep these platforms up and running, making the O&M systems mission critical. In each IT system transformation, the greatest difficulties are often achieving the needed level of service assurance and enacting a viable O&M program, as well as moving to cloud architectures which present several more challenges.

New O&M Systems Requirements from Cloud Architectures

● O&M Pressures from Cloud Computing and Business Requirements

As more and more enterprises embrace the cloud, O&M personnel will face more pressure than ever before in achieving the rapid rollout, flexibility, scalability, and higher SLA requirements on business systems, all while working with limited budgets. When O&M is placed into the high complexity of Cloud Data Center (DC) environments saturated with massive amounts of equipment, achieving 99.95 percent quality in delivery of IT services while improving efficiency and lowering costs is the biggest challenge personnel face.

- **Guaranteeing high O&M quality:** The amount of equipment within data centers has grown exponentially, from several dozen to hundreds and thousands, or even millions of pieces, as we migrate to cloud-based DCs. The massive number of devices presents a huge challenge to achieving rapid fault positioning and isolation. Adding virtualization and distributed elasticity technologies makes the cloud DC environment even more complex which, in turn, makes O&M more difficult. Once seldom-occurring faults become the norm and system impact increases, reaching 99.95 percent quality at the user-level in the SLA is difficult to achieve.
- **Improving O&M efficiency:** Adding virtualization capabilities and open-source technologies makes O&M even more complicated. Manual operations and maintenance on a network proves too slow and the probability of error too high. Most personnel can handle from 50 to 100 pieces of equipment, which indicates that a large amount of manpower would be needed to operate any large cloud-based environments.
- **Maintaining low operation costs:** Resource utilization is typically 20 percent or less in traditional IT. That rate improves significantly when resources are moved to the cloud model. However, the very nature of personalized applications and requirements for on-demand elasticity tend to fragment resources and lead to load imbalance, making it difficult to plan capacities. As a result, planning objectives are not met, and O&M costs continue to run high.

● Service Assurances and High Availability Requirements of Cloud Architectures Create Several Unknowns for O&M Planning

To improve utilization efficiency, the resources in cloud architectures are shared, meaning that specific services and applications do not run on dedicated equipment. This approach is completely different from traditional IT models. Automated and flexible scalability strategies in cloud computing achieve a balance in terms of resource sharing, user experience, and service availability. This is a core advantage of the cloud computing model, but it also brings with it new challenges in O&M. Personnel often do not even know which piece of equipment is carrying a particular service, making it difficult to pinpoint faults. The ability to prepare for these unknowns requires more complete monitoring across the entire system to yield the needed visibility.

● Unified O&M Management in Hybrid IT Systems

The leap to cloud architectures in enterprise IT does not happen in one stride; it is a long-term, phase-in process. The difference between traditional and cloud architectures requires many different tools, which presents greater challenges to O&M personnel. Achieving unification across both IT structures and centralizing management are just two of the new issues being faced.

● Requirements for Full Automation Include Personnel to Transition from a Management to a Developmental Role

The distributed architecture of cloud computing systems features automation in resource scheduling, fault isolation, fault recovery, and other utilities. This level of automation has overturned the traditional approaches to installing and deploying IT software as well as the familiar models in service usage and maintenance. The vast majority of operations are no longer carried out by personnel but are now automated. Therefore, personnel tasks are changing from being management-focused to requiring them to build automated O&M schemes and develop tools. O&M systems are also expected to evolve.

Intelligent O&M Supports Automation in IT Systems

The key to automation is making IT systems more intelligent. Only when fully enabled with smart attributes can system scalability, fault isolation,

Ma Li

Intelligent operations and maintenance is a critical component for full automation across IT systems, including fault prevention, detection, and self-healing, as well as automated capacity management throughout the full lifecycle.

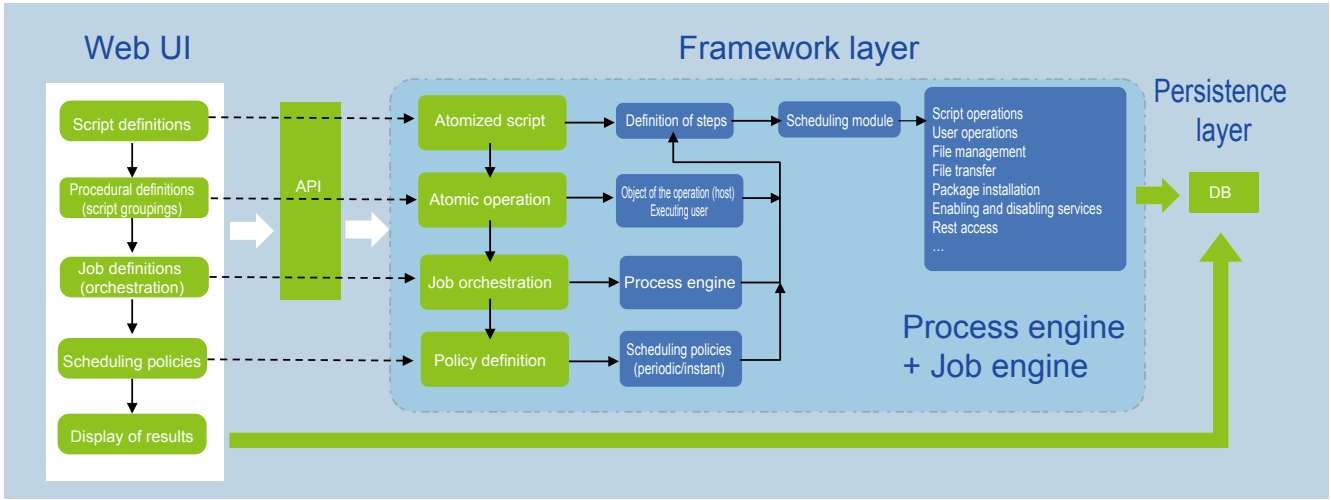


Figure 1: Automated job customization process

and restoration capabilities reach the level needed for enterprise system status, user scale, and service experience quality, as well as policy rules. Smart management and O&M systems are being relied on to deliver 1) automation in management throughout the entire lifecycle, 2) the needed intelligent fault prevention, detection, and self-healing mechanisms, and 3) wide-open flexibility in how capacities are allocated with intelligent capacity management utilities.

● Automations in Management throughout the Entire Lifecycle

The scale of resource and business capacity at cloud DCs far exceeds that of traditional layouts. If manual approaches were used to roll out, monitor, upgrade, expand, limit, downgrade, or decommission cloud-based services, the result would be low efficiency and a higher risk of operator error. Automation is imperative to improving the per-capita efficiency rating of personnel, satisfying agile service requirements, and gradually enabling the move to unattended O&M.

Automation is imperative to improving the per-capita efficiency rating of personnel, satisfying agile service requirements, and gradually enabling the move to unattended O&M. >>

- **Workflow-centric automation in service platforms simplify complicated operations:** Automated service platforms provide standardized and tool-based architectures that, through reconfigurations for high-change scenarios, are able to achieve out-of-the-box results, greatly simplify formerly complex operations, and significantly improve O&M efficiencies while lowering the incidence of erroneous operations. These high-change scenarios include rectification of known typical faults, expansions and reductions to capacities of resource pools, installation of patches, execution of health checks, compliance auditing, rectification of non-compliance issues, batch software installations, backup policies for management node configurations, extraction of configuration information, and power-on and power-off processes for large number of devices. With authority and domain-based management in addition to provisioning of operation logs, security and auditing requirements are satisfied while O&M and changes become more controllable and efficient.

In addition to making use of the common capabilities afforded from the framework, O&M personnel can customize or make changes to the automation services whenever needed. After personnel develop the atomic scripts, the scripts are then visualized and submitted. The platform can then automatically schedule and implement the various online management utilities for each service.

- **Standardized and consistent O&M approaches are key:** Large differences between the software and hardware from the various vendors in traditional DCs necessitated a lot of configurations to get the various components to work with each other as build and day-two operation complexity continued to rise, making it difficult to implement a fully viable plan. In the cloud era, the use of standard compute, storage, and networking hardware in addition to standardized software installation packages, configurations, permissions, dark launch strategies, scripts, and system health indicators enable O&M personnel to manage the entire cloud environment with the convenience of visualization and improved predictability. Self-corrections are executed according to presets to reduce risk of operator error in frequent changes.
- **Hardware plug-and-play; easy replacement:** As the scale of the data center increases, manual identification and installation of hardware become incapable of supporting rapid rollout, expansion, and decommissioning requirements. With plug-and-play technology, less-skilled personnel can install equipment on shelves, connect appliances to the network, and power on devices. The O&M system completes the end-to-end hardware system deployment and rollout according to the presets. Cloud isolation technology also allows less-skilled personnel to change out failing hardware.

Intelligent O&M platforms make use of Big Data associative analysis and machine-learning technology to deliver the needed artificial intelligence enablement for the O&M system and provide intelligent support capabilities. >>

- **One-click software deployment; always online:** With the rise of agile, distributed software development and deployment models, system upgrades are more frequent and complex in cloud DCs versus their traditional counterparts. Tools provisioned with a single click achieve automation in end-to-end deployments in everything from applying for resources to provisioning and deployment, system self-tests, service tests, rollbacks, and dark launches while supporting centralized provisioning of hundreds or even thousands of instances at multiple data centers located throughout the world.
- **Mobile O&M:** With O&M Apps available in the palm of the hand, experts can perform tasks on cloud resources from anywhere and at any time throughout the entire management lifecycle.

Intelligent Fault Prevention, Detection, and Self-healing

In traditional models, the working style for O&M personnel was to wait for faults to occur. According to statistics, the planned work for O&M staff accounted for only about 50 percent of their day with the remaining time allotted to putting out fires. With the rapid growth in scale of cloud data centers, O&M personnel need to handle a growing number of events. Using manual-intensive methodologies to put out each little fire in the system is just not a viable solution. This is precisely why intelligent O&M platforms are required. These platforms make use of Big Data associative analysis and machine-learning technology to deliver the needed artificial intelligence enablement for the O&M system and provide intelligent support capabilities in everything from fault prevention and location to closed-loop handling.

- **Active fault prevention:** No matter how fast a fault can be handled, it is still not as good as the fault never happening at all, especially in large-scale cloud DCs. Even a very low failure rate means a certain degree of impact. Prevention is the absolute best approach in avoidance of troublesome operations and those 'little fires' that keep personnel running around all day.

[Key measurement #1]: Reduce manual operation-induced faults

According to the IT Department at Huawei, manually performed change operations are the reason for over 50 percent of faults. Most level-one events are also caused by some change operation. Those types of operations tend to be rather complex, which, in turn, makes manual handling prone to error. Automating the processes avoids unnecessary faults from manual operations, which is a key measurement for reducing failure rates.

[Key measurement #2]: Implement intelligent analysis on systems to find sub-health contributors and detect potential faults early

Using Big Data technology combined with cross-domain correlation analysis on the features of the faults enables early detection and predictive analysis. Integration with the automated strategy execution system allows problems to be solved before users even know something is wrong without any interruption to services.

- **Timely fault detection:** Cloud DCs are stacked with layers of technologies and feature complex architectures, making it difficult to identify faults. Building an end-to-end monitoring system to analyze the status of all systems covering everything from resources to tenant experience helps identify sluggish response, slow query, and deteriorating device performance in service systems (frequent faults, high transaction failure rates, and so on). This type of all-around monitoring helps find the root cause of problems in low user participation and resource utilization, among other issues. The data helps technical teams continuously improve O&M management.

[Key measurement #1]: Build a fully linked, active, intelligent, and multi-indexed monitoring system to comprehensively cover all elements with multi-mechanism integrations

O&M systems need to support unified management over equipment rooms and facilities, physical infrastructures, cross-center backbone networks, virtualized resource pools, cloud services, and applications to offer centralized and multi-faceted monitoring across multiple DCs.

If a fault occurs at a data center, the current and historical operating status of each resource and cloud service at the center can be quickly obtained with the conveniences of visualization. The information that can be queried includes performance capacity, associated objects and alarms, and information on the topology and various logs.

[Key measurement #2]: Visualization of systems' statuses

Visualized display of the application topology and health status allows personnel to view operational indicators

Intelligent capacity management combines Big Data analysis and forecasting technologies to present the available capacity of physical resources and cloud-based resources in real time. >>

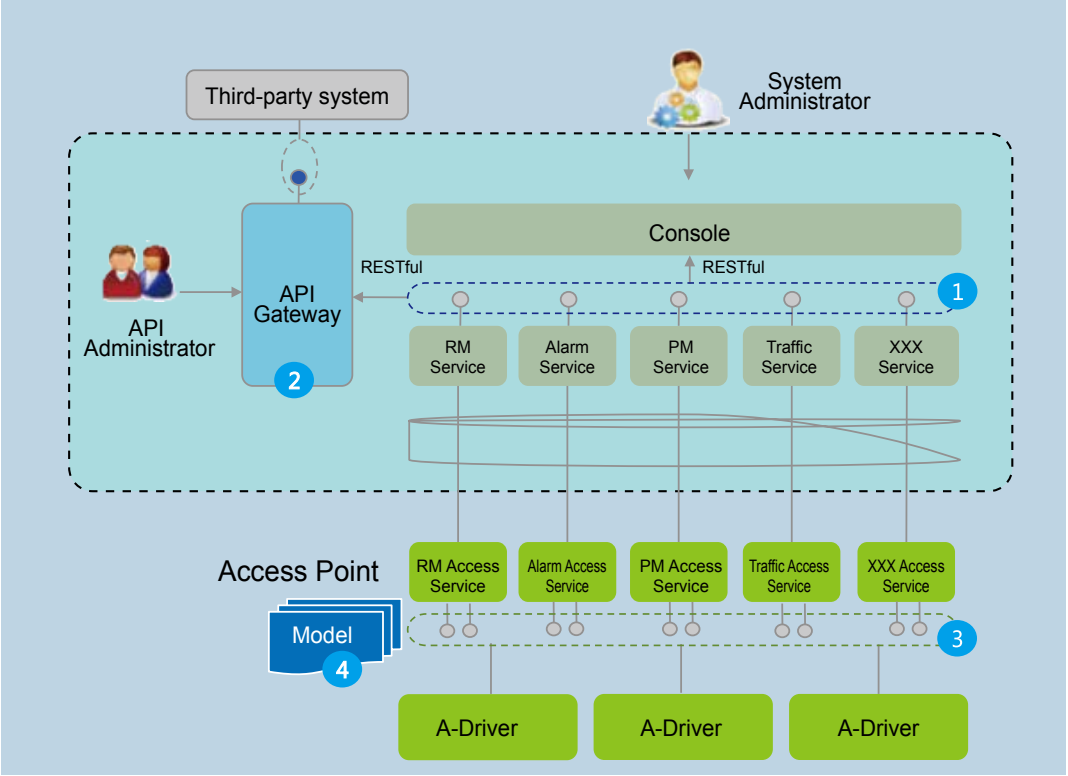


Figure 2: Open Huawei cloud O&M platform

and changes to critical services at a glance. The business application indexes we usually collect include user experience (page response speed and access performance), user behavior (number of user visits, number of active users, and maximum amount of concurrent access), business efficiency (end-to-end business processing time, transaction success rate, and the volume of supported traffic), and SLA.

IT operations personnel and administrators can use the information relating to the performance capacity of O&M items, alarm statistics and analysis, resource utilization reports, and health and capacity forecasts to generate monthly and quarterly reports on O&M quality analysis to support annual IT planning.

- **Intelligent fault locating:** The cloud era features distributed and microservice-based software architectures. The relationship between services and the scheduling that takes place is becoming increasingly more complex. This poses a great challenge to quick location of faults.

[Key measurement #1]: Use of traffic tracking systems to locate faults rapidly

To help solve the problems in the complexity of scheduling cloud-based and microservices in addition to locating faults in such environments, supplementary fault locating tools are needed to improve efficiency. Through monitoring of various metrics, the time needed to locate a fault is reduced from hours down to minutes.

[Key measurement #2]: Build an expert diagnostic system complete with intelligent fault locating capabilities, and automated recovery and processing on known faults

Routine analysis of fault summaries and the continuous accumulation into the fault feature library help experts yield intelligent fault location capabilities and automated recovery operations on known faults.

- **Automatic fault recovery:** Cloud DC expansion results in the dramatic increase in the number of faults. Huawei's experience in DC O&M has shown that, if automatic fault classification and processing are not carried out on large-scale cloud DCs, thousands of trouble tickets of varying degrees would be logged each day. Thus exists the need for O&M systems that are able to identify common faults and implement the appropriate self-healing strategy. When a fault does occur, a closed-loop strategy is automatically initiated without the need for manual intervention.

Intelligent Capacity Management Improves Utilization Rates

In traditional DCs, business systems deployed by each respective department cannot be shared, and server utilization is as low as 20 percent. Moving DCs to the cloud enables resource sharing and dynamic scheduling capabilities but brings challenges such as fragmentation, load imbalances, and difficulty in guaranteeing SLAs.

Intelligent capacity management combines Big Data analysis and forecasting technologies to present the available capacity of physical resources (server, storage, and network devices) and cloud-based resources (VMs, block storage, and so on) in real time. Utilities are also able to capture

snapshots of capacity, the loads on devices, and an overall view on fragmentation. Traditional O&M is unable to migrate or dynamically expand capacities, resulting in unbalanced loads. In cloud DCs, capacity management supplies O&M administrators with information on resources with low loads and provides recommendations on adjustments. In traditional layouts, resource fragmentation often leads to utilization efficiencies as low as 20 percent while other silos are running out of resources. Capacity fragmentation management in cloud-enabled centers provides O&M administrators a view on the physical distribution of the various types of resources as well as recommendations on resource tuning, which provides greatly improved utilization rates of existing resources.

When the utilization of cloud resources reaches a certain threshold, planners need to start thinking about expansion. Traditional approaches to forecasting the required capacity mainly relied on the limited experience of individuals and the limited amount of data that could be imported to help derive a trend. From there, a forecast was made on how much capacity could actually be created. To be safe, planners usually overshoot the capacity, causing 20 percent to 30 percent of resources to remain idle. In contrast, intelligent capacity management combines data on resource capacities, application behavior analysis, performance, financial information, and other dimensions to provide accurate predictions on how the various types of resource capacities applications used in multiple business departments will impact the IT infrastructure. Planners then have a much clearer picture of the resources required for the future as they formulate effective procurement and expansion plans.

Intelligent capacity management achieves improved visibility into resource status, the ability to observe and track issues, identification of risks, and measurable and adjustable controls to improve the resource utilization rate to 70 percent or more.

Results from O&M Practices at Cloud DCs

More successful approaches in cloud DCs apply automated and intelligent O&M systems. The advancements achieve impressive improvements in O&M efficiency, all while ensuring 99.95 percent or higher quality in services at the user-level. In traditional O&M approaches, each technician could manage 50 to 100 devices. Now, each technician can manage 5,000 to 10,000 devices (a 100-fold improvement). Overall, resource utilization has also improved from as low as 20 percent to 60 percent to 70 percent, a 300 percent improvement (Table 1).

In one example, Huawei's R&D department was able to improve resource utilization from 10 percent in many cases to 40 percent to 50 percent using only 11 people to maintain 100,000 devices with the use of standardized, automated, intelligent O&M.

At the same time, the introduction of an automated, intelligent, visualized O&M platform allows personnel to break away from mechanical, repetitive, and low-value tasks while lowering incidences of human error in processing, which indirectly helps protect the quality of IT services and lower operational costs. More importantly, O&M personnel are freed up to take part in higher value tasks, such as architectural design and development in addition to assessment and the introduction of new technologies to better support business innovation. IT teams and individuals can create more value for the enterprise by applying automated and intelligent O&M platforms that also help standardize IT management processes with the use of tools. With this automation, the entire O&M process becomes standardized, and compliance is improved to ensure SLAs are met to support the healthy development of business.

Best Practices in Huawei O&M Solution Deployments at Cloud DCs

In addition to helping enterprises build an automated, intelligent, and visualized O&M platform, the Huawei Cloud Data Center solution leverages the telecom team's many years of expertise and explorative achievements in new technologies.

- Accumulation of O&M Expertise, Commercialization of O&M Capabilities

Huawei's internal O&M teams are responsible for maintaining the massive scale of the Huawei Enterprise Cloud and

	Traditional O&M	Cloud-enabled O&M	Improvement
Average per technician	50 to 100 devices	5,000 to 10,000 devices	10,000 percent
Resource utilization	As low as 20 percent	60 percent to 70 percent	300 percent

Table 1: Improvements in O&M efficiency

“Huawei's R&D department was able to improve resource utilization from 10 percent in many cases to 40 percent to 50 percent using only 11 people to maintain 100,000 devices with the use of standardized, automated, intelligent O&M.” >>

> High-risk and high-frequency operations require automation. Huawei's self-operated enterprise cloud employs the DevOps model to rapidly build up and improve on O&M capabilities. >>

its own private cloud. These teams are also responsible for monthly O&M quality analysis as well as statistical analysis and summaries on faults. High-risk and high-frequency operations require automation. Huawei's self-operated enterprise cloud employs the DevOps model to rapidly build up and improve on O&M capabilities. After being fully validated, O&M capabilities are commercialized and included in the baseline version of the Huawei Cloud O&M solution to make the best practices available to our wide customer base. For example, the ECS service calls upon tracking tools, as one of the methods for accumulating experience from routine O&M, to integrate capabilities and improve the platform.

Opening up Capabilities to Build up the Cloud-based O&M Ecosystem

The developer community for cloud-based O&M that Huawei operates opens up APIs used at several layers to meet the application development requirements of various use cases. The community allows partners to participate in the accumulation of capabilities, enrich tool catalogs, and enhance the components going into the O&M offerings, thereby strengthening the cloud-based O&M ecosystem.

- **Opening up the service layer:** All interfaces on the service console are opened up to secondary development so third parties can customize interfaces and portals to suit various industry use cases.
- **Opening up the backend service layer:** All O&M services are opened up to secondary development through API gateways to permit third parties to develop new O&M tools or allow the Huawei offerings to connect to third-party O&M tools and systems. For example, field-specific service topology views can be developed from alarm and resource management utilities opened up for further development, which also yields visualization of service node status. In hybrid IT architectures, performance capacity, configuration information, and logs can all be linked to the customer's centralized O&M management platform through API gateways to deliver an O&M system complete with global sharing capabilities.
- **Opening up the access layer:** Provisioning of south-bound drivers in the plug-in framework allows third parties to develop their own device drivers. New device objects can be accessed through the dynamic capabilities in driver management. The driver developed by ZOHO, for example, is used to execute monitoring and report management on non-Huawei equipment.

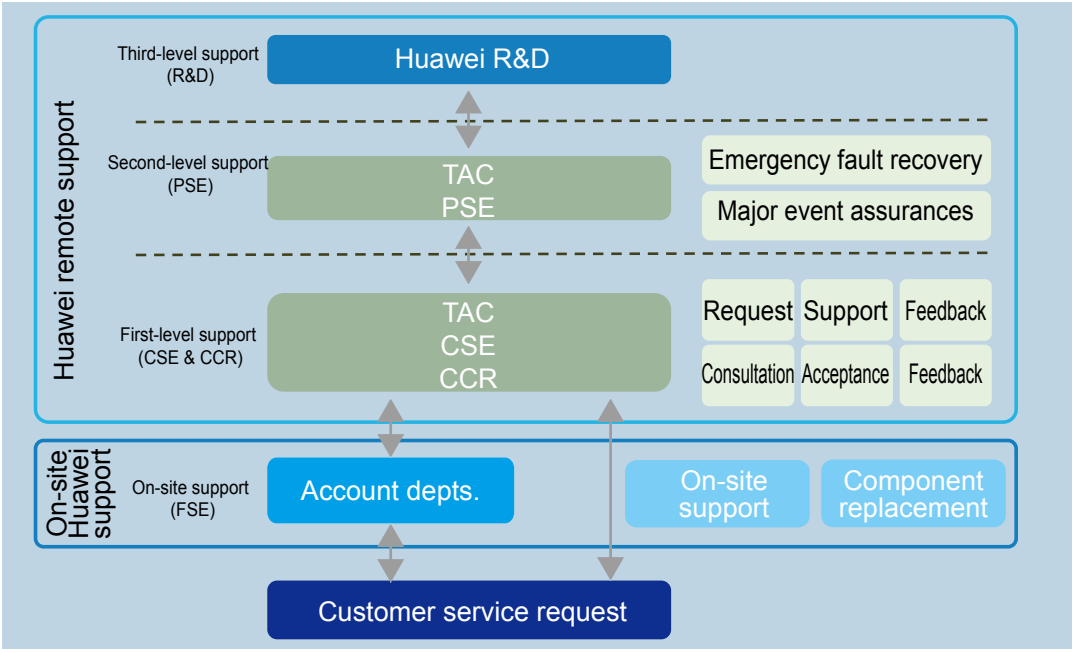


Figure 3: Technical support system

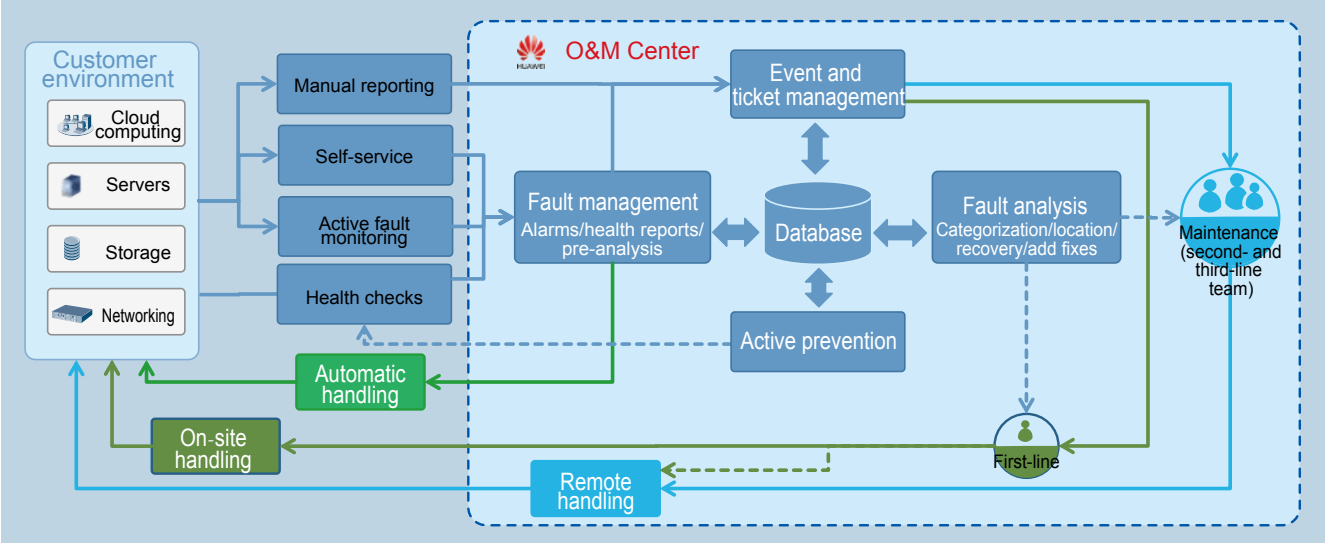


Figure 4: Intelligent O&M platform

- Microservice Architecture and Container-based Deployments

Huawei cloud O&M systems adopt a microservice architecture in support of container-based deployments, enabling agility in delivery and contributing to excellent scalability. Agility in delivery means each microservice is independent development, released, and updated for quick iterations. Excellent scalability means flexible expansion of each microservice, which, in turn, helps to ensure ease in scalability for the entire O&M system; minimal amounts of resources can be deployed during the beginning and grown on demand. Container-based deployments significantly reduce the costs in managing nodes.

- Global Technical Support System

Huawei has engaged in the communications technology field for 28 years, serving the carrier domain throughout the world. Huawei has established a complete technical support system comprising two global technical assistance centers and numerous regional technical assistance centers. The company has trained teams of highly skilled experts around the world to work in its technical support system that spans the globe.

Huawei offers a wide range of O&M models for customers to choose from, including customer-managed O&M, Huawei-managed O&M with on-site personnel, or Huawei-assisted remote O&M. Customers opting for the self-managed model can still avail themselves of the 24/7 customer hotline, deploy Cloud Service to enable automatic fault reporting and troubleshooting, and make use of the Huawei eCare tool to monitor all processes and ensure timely solutions to customer problems.

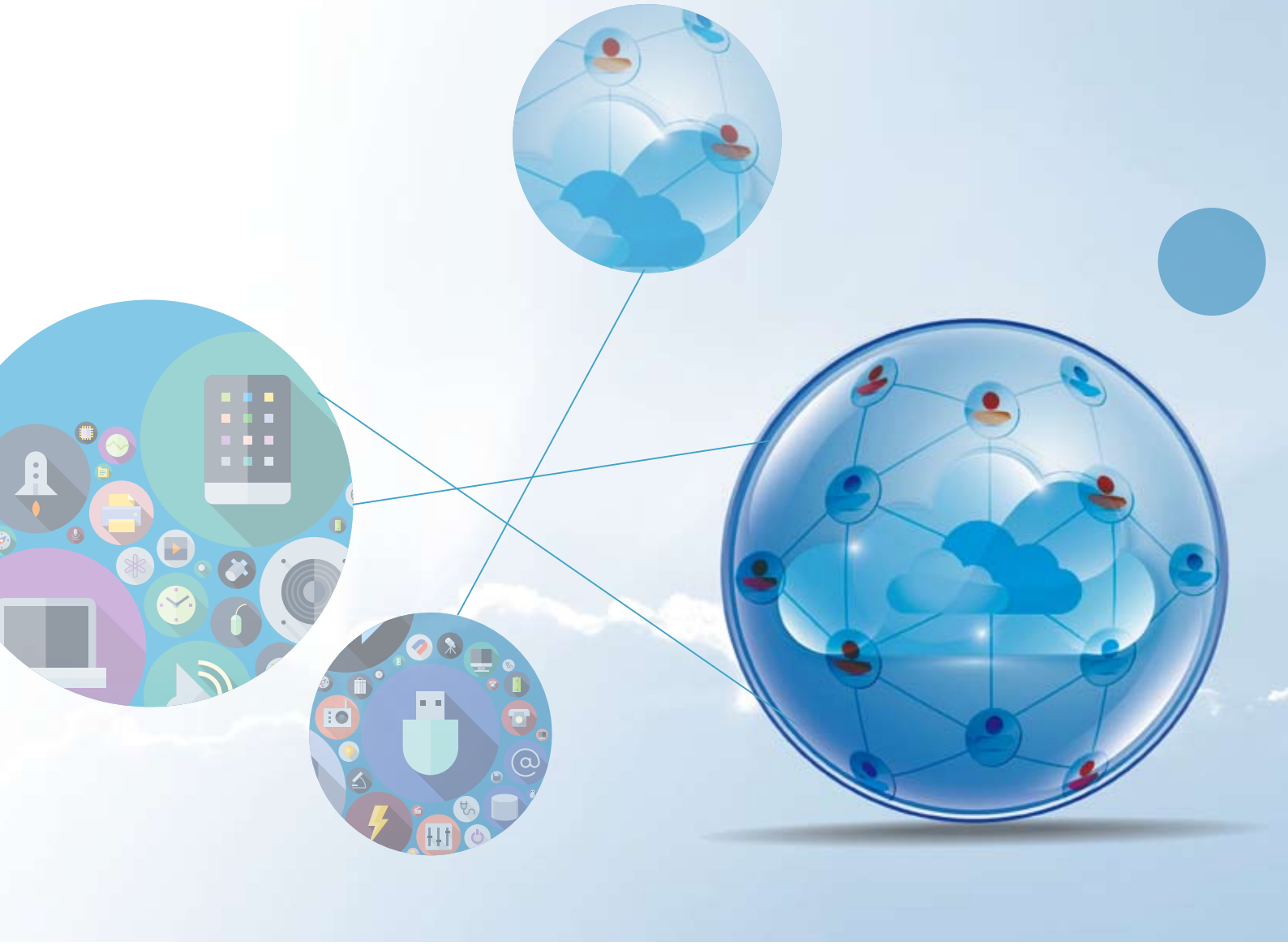
- Support for Full-stack Management

With its extensive expertise in the O&M field of ICT infrastructure and leveraging the total advantages of its own product line, Huawei delivers complete cloud DC management capabilities covering everything from servers and storage equipment to networking, virtualized resources, and cloud-based services and applications. Full-stack management paves the way for end-to-end service monitoring, fault diagnosis and locating, and automation during the entire lifecycle, among other capabilities.

In the last three years, the scale of Huawei's cloud-based DCs has increased several times over. The O&M solution has reached a 99.6 percent SLA fulfillment rate with less than 10 percent increase in O&M personnel. The average utilization rate of computing resources has reached over 50 percent, better supporting agile development in R&D. In one instance, the planned maintenance and version upgrade to DCs during the 2016 National Day holiday in China involved 11 equipment rooms across the country with a total of 15,000 physical servers and 300,000 VMs. If traditional O&M approaches were used, each engineer would have been able to handle only 3,000 to 4,000 VMs, which would have required more than 100 employees. With the power-up and power-down in a single click and the batch version upgrade capabilities of the intelligent O&M platform, fewer than 20 people were needed and the necessary time to power up and power down each equipment room was cut in half (from 10 hours down to 5).

Cloud-based O&M is an essential part of any cloud computing layout. The importance continues to grow as these platforms are becoming a core competitive strength. As a next step, Huawei will increase investments in artificial intelligence applied to cloud-based O&M and extend the inclusion of robotics at DCs in more O&M use cases to replace the traditional approach in manual operations. All these investments are aimed at providing customers with a highly automated and intelligence-infused cloud DC O&M solution able to achieve at least limited 'unattended' operations. ▲

Huawei will increase investments in artificial intelligence applied to cloud-based O&M and extend the inclusion of robotics at DCs in more O&M use cases to replace the traditional approach in manual operations. >>



Carriers Enabling **Enterprise Digital Transformation**

By *Zhang Haibo*

Zhang Haibo

In partnership with carriers around the world, Huawei is clearing the path for ICT transformation across governments and industry with advanced solutions for connected networks, computing platforms, and cloud services.

The era of a digital economy driven by new technologies, such as cloud computing, Big Data, and the Internet of Things (IoT), is rapidly approaching. The powerful trend of digital transformation is sweeping across the world. Uber owns no vehicles, but it is the world's largest taxi company. Uber changed the way people commute and has become the most popular taxi company. Adidas uses 3D scanning and printing technologies to customize running shoes in its European stores. By inserting sensor chips in each pair of shoes to collect data in real time, Adidas aims to continuously improve products in order to provide better services for their customers. This new digital era will reshape the global economic structure and business landscape, affecting all enterprises and industries. Enterprises can only choose to embrace these trends in order to deal with the new challenges brought by the transformation.

Enterprise Digital Transformation: A Long Journey Ahead

What is a digital enterprise? The interpretation varies in different industries. For example, the digital transformation of the retail industry focuses on the integration of online and offline services, uses Information and Communications Technology (ICT) to streamline product supply, warehousing, logistics, and sales phases, and provides personalized and customized services based on Big Data and consumer insight, thereby building a full-channel services mode. The digital transformation of the traditional financial industry is manifested by the digitalization of customer information, currency, products, marketing, and services. The goal is to build a smart digital financial operations platform that can widely interconnect with and be integrated into the operating scenarios of each industry's ecosystem and meet customized requirements.

Although enterprises from different industries have various requirements on digital transformation, some common features can be found. The development strategies and operating modes of digital enterprises are customer-centric. Digital enterprises build a platform using digital technologies, such as cloud computing, Big Data, and the IoT, and establish new operating modes that can adapt to the Internetization and decentralization era, thereby driving the transformation and innovation of their businesses.

The digital transformation of enterprises is unstoppable but not easy to carry out. Enterprises need to reconstruct their business, marketing, and service models to drive the reconstruction of internal management, R&D, operations, and production processes, thereby reconstructing the organization, culture, and operating concepts of enterprises. For traditional enterprises, digital transformation is doomed to be a journey full of thorns.

In the trend of enterprise digital transformation, the first challenge for the Chief Information Officer (CIO) and Chief Digital Officer (CDO) is how to build a digital platform using new digital technologies. First, the fragmented connection must be resolved. The digital platform cannot only realize the full connection between people and people, things and things, and people and things, but can also connect enterprise employees, customers, partners, suppliers, and the suppliers of suppliers, so as to break down information silos, allow for better data flow, and ensure the core data security of enterprises. Second, agile enterprise IT must be built using new technologies, such as cloud computing and Big Data, to meet the demands of digital enterprises for agile delivery and provide Real-time, On-demand, All-online, DIY, and Social (ROADS) experiences for customers, partners, and employees. Finally, a digital ecosystem that can cross industry boundaries for wide integration needs to be constructed to produce innovative business models.

Carriers: Indispensable in the Digital Wave

According to International Data Corporation (IDC), by 2018, digital transformation will be the key strategy for 67 percent of the top 2,000 global enterprises. By end of 2017, over 50 percent of the enterprise IT budget will be spent on new technologies. According to Saugatuck Technology, by 2018, more than 60 percent of enterprises will migrate over half of their infrastructures to a cloud platform. Therefore, the cloud computing platform will become an ideal choice for enterprise digital platforms and will constitute the new-generation enterprise IT infrastructure.

In the wave of enterprise digital transformation, global telecom carriers that own global networks and communications infrastructures are bound to play an indispensable role. Among cloud service providers, telecom carriers have the most complete data centers and network resources distributed across the world, carry 80 percent of the global data traffic, and provide carrier-class security standards. With these advantages, the globally distributed public cloud services of carriers can enable the IT infrastructure (cloud computing) to be used on demand and expanded elastically like public services, such as water and electricity, providing enterprises with agile IT. Public cloud services also have the following advantages.

- Full Connection Capabilities

Carriers own network resources distributed globally. Based on the network resources and services provided by the cloud platform, such as Bandwidth-as-a-Service, Direct Connection, cloud Virtual Private Network (VPN), and Security-as-a-Service, enterprises can quickly construct a globalized network, connect customers, suppliers, distributors, transaction service providers, and industry partners in the digital ecosystem, and resolve the fragmented connection problem, allowing for rapid data collection and flow to provide real-time and online support for digital services.

With the development and application of IoT technologies, data will grow exponentially. By 2020, it is estimated that over 200 billion sensors will be distributed on about 30 billion terminals. Over 25 exabytes of data will be generated per month. However, the existing 3G and 4G networks cannot support such massive amounts of data. Carriers need to deploy 5G or higher transmission rate channels to provide ultra-wide data pipes to support digital transformation. In addition, with the IoT technology, carriers construct the IoT platform based on the cloud platform. The IoT platform provides connection, data collection, network transmission, data storage, and data analysis to help enterprises fully connect people and people, things with things, and people and things, as well as integrate and share enterprise data, thereby quickly creating value and providing power for digital transformation.

- Regulation Compliance

The digital transformation of enterprises evolves data from distributed storage to centralized sharing, and resources from physical servers to distributed Virtual Machines (VMs). Data will become the core asset of enterprises, and data security will become the toughest task for enterprise CIOs. Remote access to a large number of Internet terminals blurs the security boundary and increases the risk of data leakage and unauthorized access. How can the digital core 'data' assets be totally secure? Throughout the development history of global networks, carriers could provide the global connection services with the highest security level only when they strictly conformed to the security regulations of each country and built commercial communications networks with carrier-class security standards. The cloud services constructed by carriers with the carrier-class security standards can comply with local laws and regulations, meet requirements of data compliance, and safeguard digital transformation.

In the wave of enterprise digital transformation, global telecom carriers that own global networks and communications infrastructures are bound to play an indispensable role. >>

- Localization Capabilities

The digital transformation of enterprises has high requirements on the infrastructure, Platform-as-a-Service (PaaS), and network services, and requires end-to-end

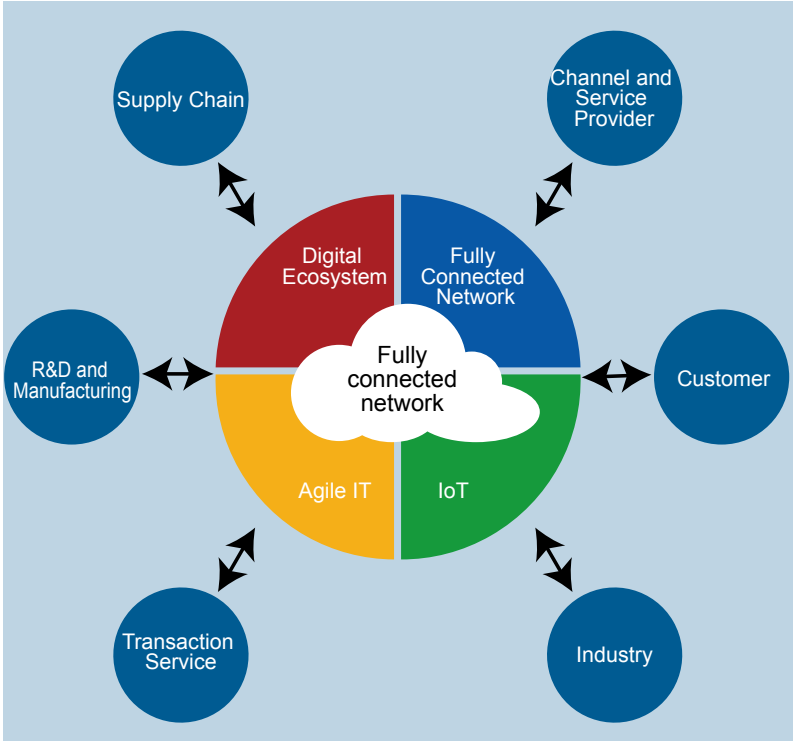


Figure 1: Enterprise digital platform model

digital transformation solutions to reconstruct the digital ecosystem. Carriers own mature enterprise service hosting and IT Outsourcing (ITO) service capabilities, serve many large-scale enterprise customers, and have experience in providing ITO services for large-scale enterprises. Carriers evolve with the enterprise digital transformation. Original enterprise services, such as Virtual Desktop Infrastructure (VDI), Enterprise Resource Planning (ERP), and collaboration and video conferencing, are gradually migrated to the cloud platform. In addition, carriers accelerate the cooperation with industry solution providers, Independent Software Vendors (ISVs), and System Integrators (SIs). With the advantage of localized services and ecosystems, carriers build end-to-end industry solutions and cloud-based implementation capabilities.

In addition, when moving to the cloud, carriers require both cloud services and professional localized services. Carriers provide professional strategic planning and consultation for the cloudification of the IT infrastructure. On one hand, carriers help enterprises migrate traditional services to the cloud. On the other hand, carriers help enterprises cultivate the ability to develop and deploy innovative applications based on Cloud Native. The localization capability of carriers can help enterprises break down technical barriers, quickly construct cloud-based, new-generation digital platforms, and enable enterprise digital transformation.

Huawei Partners with Carriers to Enable Enterprise Digital Transformation

Faced with the opportunities for enterprise digital transformation, Huawei strengthened its strategic partnerships with carriers at *Huawei Connect 2016* and aims to make joint efforts to establish a fully connected society and realize digitalization in all industries. The digital transformation trend is also a transformation opportunity for the telecom industry. The cooperation between Huawei and carriers can make up for the shortage of carriers in ICT developments and research capabilities, improve end-to-end solution proficiencies for the whole industry, and help them support enterprise digital transformation.

Huawei builds an open cloud-pipe-device collaborative platform that is resilient, flexible, and secure, and will make all efforts to provide comprehensive support for telecom carriers in 5G, cloud computing, the IoT, Big Data, and video technologies. For cloud computing, Huawei supplies strong R&D and service delivery capabilities. With its cloud computing platform based on the advanced OpenStack architecture and integrating Huawei's technology advantages, such as server, storage, and network, which ensure the openness of the platform and provide business-level service assurance for Huawei and carriers. In terms of the IoT, Huawei provides carriers with complete IoT solutions from the protocol layer to the transport layer, and then to the platform layer. Huawei has cooperated with companies, such as agricultural equipment and elevator manufacturers HOLMER and the Schindler Group, respectively, to develop customer services based on the IoT technology. Huawei provides Big Data and video technologies for users of PaaS services on cloud computing platforms to help enterprise digital transformation.

Huawei will cooperate with world-renowned carriers and partners to establish an open and win-win digital ecosystem, covering the infrastructure, digital platform, and end-to-end solutions. >>

In addition, Huawei offers industry-leading ICT innovations and has rich experience in providing industry-oriented, end-to-end digital solutions as well as building industry ecosystems for government, electricity, energy, finance, education, retail, and public security sectors. By partnering with carriers, Huawei integrates its enterprise-oriented ecosystem and solutions with carriers' service capabilities and localized ecosystems, creating comprehensive solutions and capabilities toward enterprise digital transformation. Currently, Huawei cooperates with carriers in multiple industries. In Europe, Huawei works with carriers and vendors of software, such as Computer-Aided Design (CAD), Computer-Aided Engineering (CAE), and ERP in the automobile industry, to create end-to-end digital solutions for automobile manufacturing based on the cloud platform. Huawei joins hands with carriers to create industry digital transformation cloud solutions, helping enterprise digital transformation.

Furthermore, Huawei will cooperate with world-renowned carriers and partners to establish an open and win-win digital ecosystem, covering the infrastructure, digital platform, and end-to-end solutions. Huawei hopes that it can play a positive role in the ecosystem and develop together with partners.

We believe that the cloud platform built by Huawei and leading global carriers is sure to boost the enterprise digital transformation of various industries. ▲

Agile Network **Wins Cloud Future**

By *Swift Liu*

Although 'past success provides no sure guide to the future,' summing up the past is undoubtedly the basis for looking ahead, especially in the technology sector. Over the past two decades, the network world has undergone three major changes. The first change is featured by fast growing network speed that increased by a hundred times every decade, from 10 Mbit/s to 1 Gbit/s to the present 100 Gbit/s. The second is the convergence of network technologies, from the previous diversity of Ethernet, Frame Relay, TDM, ATM, and POS to the current Ethernet and IP. The third is the emergence and maturity of SDN, gradually extending from data center that supports cloud computing to WAN and campus networks. SDN has the typical IT characteristics and is actually driving the evolution towards an IT-oriented network, which will be unstoppable once started. In other words, an IT-oriented network is the future. So what's next after SDN?

Swift Liu

Huawei's CloudCampus Network solution promises to deliver enterprise networking on demand, plus self-services and automated tools that require minimal management, yet ensure security and reliability.

The Cloud Brings New Opportunities for the Network

Over recent years, the cloud has tremendously impacted the transformation of networks. In a sense, networks served to support the implementation of the cloud. Since the cloud itself is also important for future IT, we use it as a technical means to optimize existing networks. Networks of the future will be 'for the cloud and by the cloud' to create availability whenever needed and automatically provision services that require minimal management, while ensuring security and reliability.

For example, according to a report published by Gartner, the primary challenge for the current campus network is that high OPEX accounts for around 73 percent of the network TCO. Therefore, an effective reduction in OPEX is the key to improving the network operating efficiency.

To date, the biggest change to campus networks is wireless access on the network edge. As the number of network devices grows and the demand for greater Wi-Fi access increases, the coverage of a campus network usually requires thousands of Access Points (APs). For instance, Huawei has deployed over 3,000 APs for the campus network of the U.K.'s Newcastle University, while the wireless coverage of student dormitories in China's Tsinghua University requires over 10,000 APs. The deployment of these APs needs complex planning and optimization based on traffic and location. If these devices are managed and configured in the conventional way, the workload can be enormous.

Another change is the continuously increasing north-south traffic over the campus, as the contents tend to converge in the data center and the cloud. For example, the large amount of Wi-Fi accesses will bring changes in traffic as the users' locations change in such cases as students moving between classrooms for different courses, employees flocking to the cafeteria from the office at lunchtime, and users flocking to shopping centers in a Wireless City after work. As access locations change, some traffic will temporarily become east-west traffic within the campus. Ideally, in the future, the network can be optimized in advance based on the changes in traffic patterns and access locations in order to provide users with the best experience.

Moreover, the campus network is turning from a conventional network that simply supports office connectivity to a comprehensive network that enables new services like video surveillance and the IoT. Meanwhile, the devices accessing the campus network tend to be complex. However, how can we quickly determine whether a problem is in the network or the end devices?

Campus networks nowadays have increasingly higher requirements on the competence of maintenance engineers, who are expected to master not only the conventional equipment such as the switches, routers, and security gateways but also various components including Wi-Fi, SDN, NFV, video surveillance, and the IoT. Ultimately, the employee competency model will evolve towards a full-stack engineer, and the personnel costs will naturally rise.

In the IT field, businesses can adopt the public, private, or hybrid clouds to reduce costs and improve efficiency, due to the concentration of resources, maintenance, and talent. The

In the IT field, businesses can adopt the public, private, or hybrid clouds to reduce costs and improve efficiency. The question is: Can we make similar use of the cloud in the network field? >>

question is: Can we make similar use of the cloud in the network field?

Network Cloudification Is the Future

Following the above idea, Huawei has proposed a new CloudCampus solution.

In 2013, Huawei released an SDN-based Agile Campus solution, whose major components include an Agile Controller and a new generation of switches, the Agile Switch series. Over the past two years, more than 1,000 Agile Campus solutions have been deployed on live networks.

In the SDN-based solution, the SDN controller is deployed locally. In the new CloudCampus solution, Huawei deploys all types of management components on the cloud to implement and manage campus networks. On such a cloud campus network, deployment, O&M, configuration, management, and inspection are automatic, and professionals are centralized to serve more equipment and customers, thereby reducing costs. At the same time, the skill requirements of field personnel are lowered, minimizing OPEX.

In addition to the SDN controller, network management system, and various Value-Added Services (VAS), there are some other specialized tools integrated on a cloud platform and accessible to more people, thereby achieving service rollout in minutes, and saving labor costs in O&M by over 80 percent. On top of that, the entire architecture is open, facilitating secondary development.

Huawei's CloudCampus solution has three highlights: all scenarios, all business models, and the full lifecycle.

- **All scenarios:** Huawei's CloudCampus solution is suitable for branches and Small and Medium-sized Businesses (SMB), and even large enterprise campuses. A full range of campus network equipment (not just basic equipment like Wi-Fi) is supported.

So far, the market has seen no cloud management solutions that support medium-sized and large campuses. This is because cloud management for a large campus has to support more devices and more complex network topology, which is technically difficult.

From the product perspective, Huawei's CloudCampus supports not merely a simple combination of Wi-Fi and gateway devices but also all categories of network products, including switches, routers, WLANs, security equipment, and IoT products.

In June 2016, Huawei released the first version of the CloudCampus solution, now available on Huawei's public cloud at Naas.huawei.com. This version can manage the customer's branches and small campuses, and deployment is under way by some customers, including automobile dealerships, retail stores, and hotels.

By the end of August 2016, Huawei released the second version, which supports up to 100 models of network equipment, including Wi-Fi, access routers, and switches, as well as security products such as firewalls and next-generation firewalls. It can be used for cloud management of branches and small and medium-sized campuses.

In 2017, Huawei will release a new version of CloudCampus, which supports more products and larger campus networks.

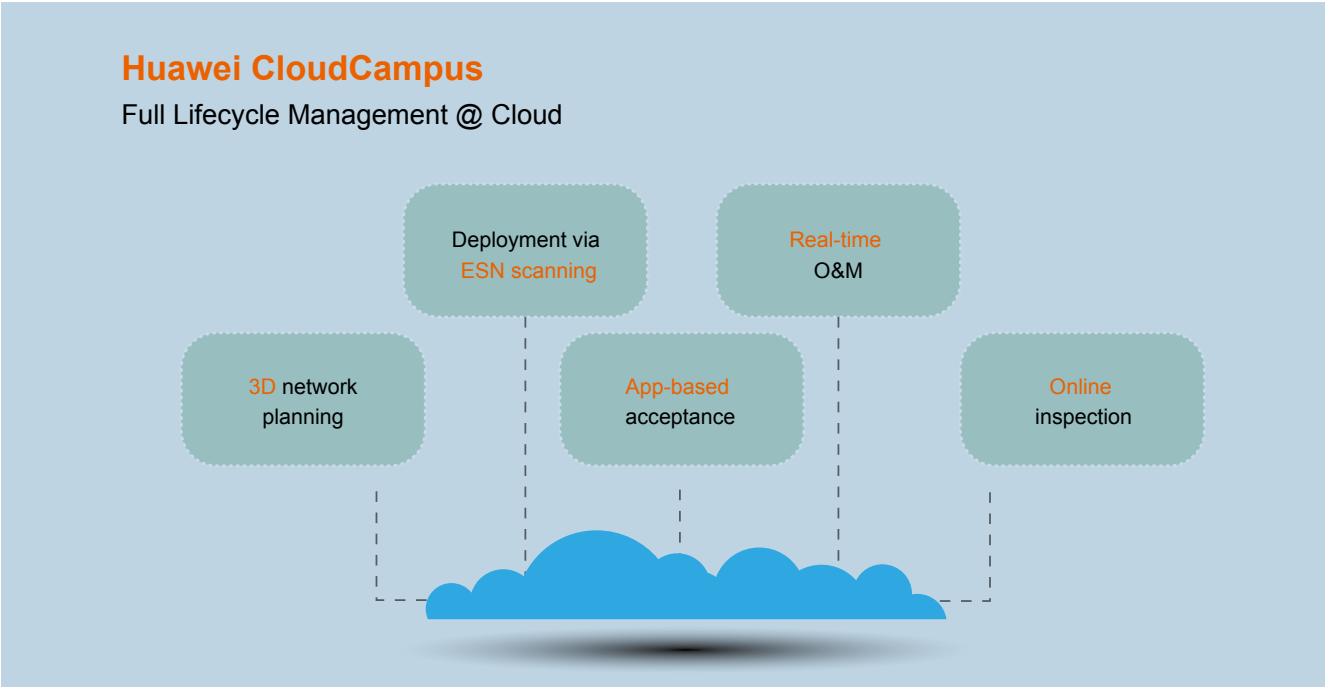
- **Full lifecycle:** Network planning, deployment, configuration, optimization, upgrades, and inspection are all performed on the cloud.

Huawei's CloudCampus solution offers a network planning tool on the cloud that automatically generates the planned topology and Wi-Fi deployment locations and signal strength graphs after the planning personnel input the network layout. This simplifies network planning.

In the deployment stage, specialists are no longer required for the field installation. Through the scanning of equipment codes with mobile Apps, the configuration can be automatically downloaded to the devices to complete automated deployment.

For acceptance of projects and networks, especially wireless networks, mobile Apps and the cloud can be used in combination to complete the necessary inspection reports.

For O&M, the cloud provides a dedicated platform, on which online inspection, diagnostics, and fault location and rectification can be performed. Specialists are also available on the cloud to help locate and rectify faults via phone calls or Apps.



• **All business models:** Huawei's CloudCampus solution supports the following three types of business models.

In the first model, Huawei runs cloud-based network management services, and partners sell products and services to end users. Huawei does not have to deal directly with the customers. This model is now available.

In the second model, Huawei sells platforms and products to the Business-to-Business (B2B) departments of telecom operators or major Managed Services Providers (MSPs), who then provide cloud management services to end users. These B2B departments and MSPs now expect to transform from merely implementing projects to delivering projects, managed O&M, and services in the cloud era.

Such cloud management solutions are still unavailable for large campuses on the market. So, they have to play the role of an intermediary, selling products and services for others. Huawei's CloudCampus caters to the specific needs of these B2B departments and MSPs, who may provide services for end users on this basis.

The third model is similar to the cloud management mode of private clouds. For some big companies like Huawei, it may be imprudent to entrust the management of their own campus networks to others, especially in the initial stage after their campus networks are launched. Huawei CloudCampus solution can also be sold to these customers, enabling them to operate the platform like running a private cloud, so as to reduce the difficulties in management, deployment, and operation and, therefore, decrease costs. That is to say, the CloudCampus solution can be either rented or purchased by the users.

> Huawei's CloudCampus solution is just a typical cloud-based campus network. In fact, the cloud is evolving and is about to change the landscape of enterprise leased-line and optical networks. >>

There is one more question: Does the previously purchased Huawei equipment support cloud management? The answer is yes, and the user can smoothly switch between cloud management and non-cloud management environments.

What Is Past Is Prologue

A quote from Shakespeare may be of benefit to our understanding of Huawei's network cloudification strategy, which reads 'What is past is prologue.' Huawei's CloudCampus solution is just a typical cloud-based campus network. In fact, the cloud is evolving and is about to change the landscape of enterprise leased-line and optical networks.

As we step into digital transformation, perhaps the CloudCampus solution is just one small step towards network cloudification, but its subsequent impacts can constitute a giant leap in enterprise digital transformation. Huawei is committed to moving forward with partners and customers to embrace a better digital future.▲

Delivering a Borderless Collaborative Experience with Enterprise Cloud Communications

By *Ma Haixu*

Kevin Kelly, former executive editor of *Wired* magazine, predicted and depicted the future of businesses in his 1994 book, *Out of Control*: Enterprises will evolve into an ecology, and different ecologies will form a borderless, centerless, open social business environment like a tropical rainforest. In the future business ecology, different groups will be fully connected into a swarm that collaborates to conduct business activities with high efficiency.

Over the past two decades, with the rapid development of Information Technology (IT) and the combination of the Internet, mobile communications, and cloud computing, tremendous changes have taken place in the ways people obtain, exchange, and process information. Innovative communications methods and tools, such as online phone calling, video-conferencing, and cloud video streaming, keep emerging. Communications within an enterprise, between enterprises, and between enterprises and customers are no longer subject to restrictions in time or space. Kevin Kelly's prediction is gradually coming into reality.

At the moment, there are still a lot of problems and challenges that impede the construction of an information-based enterprise. The implementation of efficient collaboration is hindered by various factors, including closed communications systems, high maintenance costs, poor business experience, and low scalability. The establishment of efficient communications and the progress of digital transformation will be vital in enhancing the core competitiveness of businesses.

Focusing on cloud, convergence, and openness, Huawei has launched a one-stop Enterprise Cloud Communications solution to support the requirements of businesses for future-oriented communications and digital transformation by delivering a borderless collaborative experience that helps enterprises achieve efficient collaboration and business agility. The solution allows enterprise communications to advance from on-premises to on-cloud, from internal users to partners and customers, and from office to production.

All On-Cloud Empowering Borderless Service Access

The cloud is driving a comprehensive digital transformation of enterprises. The conventional IT infrastructure has been gradually migrated to the cloud, creating favorable conditions for enterprise communications to embark on a journey towards the cloud. Based on cloud technology, Enterprise Cloud Communications can achieve agile deployment of services, flexible scale-up/-down of resources, automatic service orchestration, and fully automated Operation and Maintenance (O&M), providing enterprises with quick and cost-effective access to communications services.

- **To eliminate the boundaries of hardware,** communications software can run on the existing general-purpose hardware (data center), sparing enterprises the need to go through a long cycle to purchase dedicated hardware.
- **To eliminate the boundaries of time,** communications systems can be rented, instead of purchased, and subscribed instantly on demand, enabling enterprises to swiftly build their own communications and collaboration platforms.
- **To eliminate the boundaries of communications costs,** service portfolios can be flexibly selected to instantly adapt to the changes in business scale; asset-light communications operations can be achieved without the need for a specialized IT maintenance team, allowing enterprises to focus on their core businesses.
- **The enterprise's demands for communications may vary at different stages of development,** and choice should be made flexibly between the options of public, private, and hybrid clouds. Enterprise Cloud Communications solution enables multi-cloud collaboration, which delivers interoperability, license sharing, consistent experience, and smooth migration of services and applications between the public and private clouds, empowering seamless scale-up/-down of services.

Practice shows that, by removing the lengthy processes of purchase, installation, configuration, and rollout, Huawei's Enterprise Cloud Communications solution has been able to help enterprises reduce product rollout time and O&M costs by 80 percent.

Guangdong Telecom, for example, provides over a million small and medium-sized enterprises in the province with Enterprise Cloud Communications services that feature flexible deployment, on-demand sub-

Ma Haixu

Focusing on cloud, convergence, and openness, Huawei has launched a one-stop Enterprise Cloud Communications solution to support the requirements of businesses for future-oriented communications and digital transformation by delivering a borderless collaborative experience that helps enterprises achieve efficient collaboration and business agility.

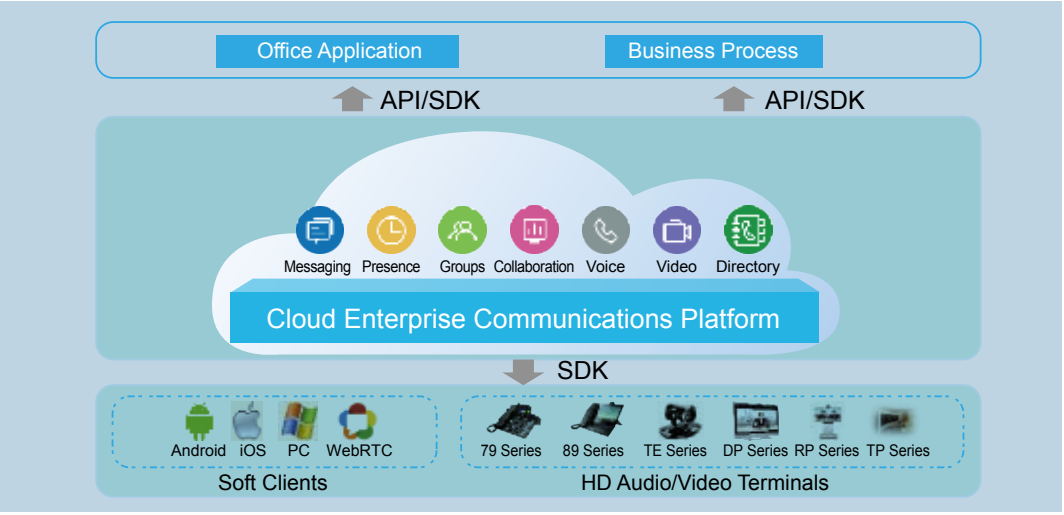


Figure 1: Huawei's one-stop Cloud Enterprise Communications Platform

> The Huawei Cloud Enterprise Communications platform connects people, processes, and knowledge, helps with convergence of multimedia, convergence of the office, and convergence with partners and customers. >>

scriptions, and minimal O&M. All these cloud services are offered through optical fiber connections, lowering the enterprise's initial investment in audio/video conferencing and Private Branch Exchange (PBX) connectivity. Thanks to easy availability and cost efficiencies, Guangdong Telecom has succeeded in expanding its user base by 40 times, increasing the stickiness of government and enterprise customers, and improving the Average Revenue Per User (ARPU).

Achieving Borderless Collaborative Office with Total Service Convergence

Jack Welch, former Chairman and Chief Executive Officer (CEO) of General Electric, envisioned that a borderless organization would remove the boundaries among functional departments and allow information to flow freely between the engineering, production, marketing, and other sectors. There would be no mental distinctions between 'domestic' and 'foreign' operations; the external barriers would be torn down to engage the suppliers and customers as part of the operation process.

Huawei's Enterprise Cloud Communications solution has reshaped how communications is conducted via the cloud in order to support for the materialization of borderless business. The solution helps with convergence of multimedia, convergence of the office, and convergence with partners and customers. The Huawei Cloud Enterprise Communications platform connects people, processes, and knowledge.

- Omnimedia Convergence

On one unified client, communication will not be interrupted at any point during the process of one-click switching from instant messaging to voice and video calls to multimedia data conferencing. The seamless communication and smooth scaling of function will deliver unhindered service experiences.

The meeting system is also becoming increasingly smarter. When participants enter the conference room, the system will recognize them and automatically boot into the conference mode. While the conference is under way, the camera will automatically track the speakers and show close-ups. In multinational meetings, the smart translation technology will eliminate barriers to multilingual communication. Moreover, a large touch screen allows teams at different sites to remotely collaborate in real time and perform operations such as drawing, marking, and commenting as if on a single, shared screen.

- Convergence of Office

The convergence of communications and office processes, such as Office Automation (OA), Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM), will be widely applied in process approval, contract review, and technical maintenance, making communications a platform connecting people and services.

A unified corporate directory and instant status feature will empower the staffs to view the current status of their contacts and initiate audio/video calls at any time. Via data collaboration, users who are processing a key task can initiate group meetings attended by experts to obtain their suggestions and guidance. The entire meetings can be archived by recording and screen captures for future analysis.

- Convergence with Partners and Customers

Besides improving their internal office efficiency, enterprises also need to collaborate more closely with partners and customers. Based on a unified cloud architecture, enterprise communications can break the network barriers in combination with network security policies to facilitate seamless communications between enterprises and suppliers, and between channels and customers.

For instance, aided by total service convergence and collaborative Enterprise Cloud Communications, Huawei's 170,000 employees and numerous partners around the world are able to hold 40 thousand meetings, make 400 thousand calls, and send 40 million messages per day. A better service experience is delivered, enormously enhancing Huawei's operational efficiency.

Communications-integrated Production Breeding Borderless Industry Innovation

IT is an essential element of production. The well-known consulting firm Gartner found that if Communications-Enabled Business Processes (CEBPs) accounted for 10 percent of an enterprise's businesses, the overall operational time could be cut down by 50 percent. Communications capabilities integrated in the production process will unleash the enterprise's productivity.

In production, for instance, when detecting an equipment fault, such as overheating, the system will automatically find and notify the personnel responsible for the state of the equipment by initiating a call or sending an email or instant message. This substantially shortens the fault recovery time.

Based on a system architecture that features convergence and openness, Huawei's Enterprise Cloud Communications solution totally opens up and integrates the communications capability into business processes through secondary development of enterprises and partners. The solution will promote business agility, persistently spur productivity, and advance digital transformation of enterprises.

Huawei's Enterprise Cloud Communications solution offers eight categories of atomic Application Programming Interfaces (APIs) for audio, video, conferencing, messaging, status, groups, directory, and authentication management. In particular, APIs for key sectors, including education, medical care, banking, and convergent commanding are encapsulated based on each scenario, allowing third-party partners to swiftly develop innovative services and applications in various segments.

> Huawei Enterprise Cloud Communications solution has attracted more than 100 industry partners, forming the cloud enterprise communications alliance that cooperates on more than 300 commercial projects to provide services for approximately 600,000 enterprises. >>

Huawei's Enterprise Cloud Communications solution has attracted more than 100 industry partners, forming a cloud enterprise communications alliance that cooperates on more than 300 commercial projects to provide services for approximately 600,000 enterprises across various sectors, including finance, electric power, medical care, public safety, and manufacturing. Thanks to the powerful open capabilities, the cooperation mode with Huawei setting the stage and partners putting on the show is yielding fruits in more and more regions across the globe. Huawei's Cloud Enterprise Communications platform has helped more and more partners and developers with industry innovation and implementation.

In 2015, Kevin Kelly described a promising future for cloud computing by revealing a magnificent framework, and he once again predicted that 50 percent of applications will run on the cloud by 2020. Cloud computing will be just like air to us and we cannot live without it. Although we usually do not consciously feel its existence, the sharing experience will be unprecedented and ubiquitous.

The development of the Enterprise Cloud Communications solution has just taken its first step. With the further evolution of the digital economy, enterprises and organizations will no longer exist or operate alone. Instead, everything will be connected, and everything will survive on communications and collaboration. As an engine of growth, Huawei's Enterprise Cloud Communications solution will drive more sectors to change and innovate their business models.

The future is on the way and it is worth waiting for.▲

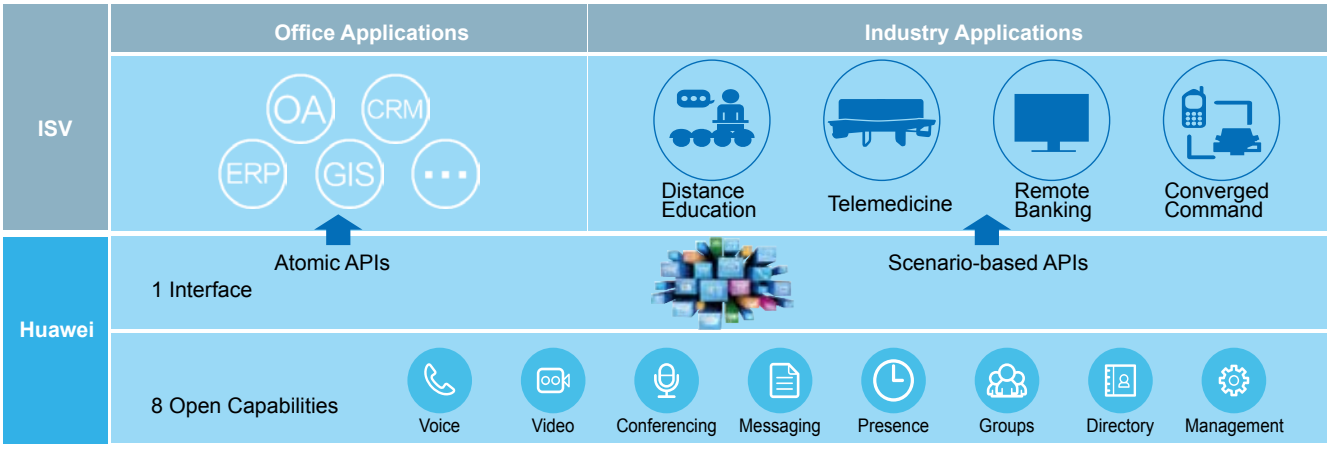


Figure 2: Open capabilities of Enterprise Cloud Communications

Building Intelligent Defense in Depth for **Trusted Clouds**

By *Yang Yong*

Every revolutionary technological change has brought challenges as well as opportunities. Although cloud computing brings effective and cost-efficient IT services to customers, it raises concerns about security. The new security challenges in the cloud era can be resolved to realize a trusted cloud only when these challenges are well understood and a comprehensive defense-in-depth mechanism is applied.

Yang Yong

Cloud Service Providers must adopt a variety of means such as technologies, compliant operations, and information transparency to handle security risks and win customers' trust. Defense using a single method can hardly secure the cloud, so a comprehensive solution is needed to build a defense-in-depth mechanism.

For customers, security in the cloud era is not only about challenges but also advantages. Large Cloud Services Providers (CSPs) have strong security teams that are capable of developing cloud security solutions based on defense in depth and responding to emergencies efficiently to better cope with security threats and assure security. The addition of customer security services has expanded the capabilities of the CSP cloud infrastructure.

CSPs may offer a wide range of security services from which customers can choose; for example, vulnerability scans, security configuration checks, and patching. Providers may also integrate top third-party security products in the industry as options for customers such as the Web Application Firewall (WAF), Data Loss Prevention (DLP), and antivirus software. However, most customers can hardly afford a sophisticated security team due to the lack of security talent and hence high costs. Key reasons for migrating advanced security services into CSP platforms are stronger security and the higher cost of engineering expertise.

Major Security Threats for the Cloud

- Data Security

On September 22, 2016, Yahoo confirmed that a 500 million-account breach occurred in 2014. The disclosure may affect Verizon's proposed USD 4.8 billion acquisition, but this is not a single case. Attackers have compromised 360 million emails of MySpace users and the information of 167 million LinkedIn accounts and 145 million eBay users.

Chief Information Officers (CIOs) in some enterprises believe that cloud services will make the data stored in the cloud more vulnerable to attacks. However, in many cases, data breaches and other attacks are incurred by ineffective authentication, the use of weak passwords, and loose management of keys or credentials.

Data protection is the top priority. Data security is so important that the industry has been focusing on data security in risk analysis and security architecture design in recent years.

- Opaque Operations on Data that Raise Concerns about Control Rights and Privacy

Enterprise customers want to be able to independently verify how their data is stored, accessed, and encrypted to eliminate their concerns about data security. After the Edward Snowden revelations, many companies not only worried that the Government could view their data but also worried that the enterprise data was accessible by cloud administrators.

Furthermore, since the location of data storage is unknown, tenants fear the data they no longer need will not be permanently erased from the cloud's physical storage devices. Huawei prioritizes user privacy protection and will not access tenant data on the public cloud. The public cloud services provided by Huawei outside China are usually operated by partners. For example, Deutsche Telekom is in charge of a public cloud. A telecom company with a good local reputation can better win customers' trust.

- Hacked Interfaces and APIs

Application Program Interfaces (APIs) and User Interfaces (UIs) are usually accessible from the Internet, which opens the system to the outside and makes them most vulnerable to attacks.

As for public clouds, tenants and Internet users can directly access these services. For example, users will log in to the web page for cloud service subscriptions. These web services are open to all users on the Internet, and hence carry great risks. Moreover, tenants could also be attackers. An attacker may be disguised as a tenant and subscribe to a cloud service in order to test the vulnerabilities in the service for subsequent attacks. Platform-as-a-Service (PaaS) is mainly provided using APIs. Therefore, inappropriate design or use of APIs may introduce risks.

- Risks Brought by Sharing Technologies

A public cloud is a big system shared by a large number of tenants. Cloud

Key reasons for migrating advanced security services into CSP platforms are stronger security and the higher cost of engineering expertise. >>

services share the infrastructure, platforms, and applications. Any component vulnerability may affect all tenants.

For example, multiple component vulnerabilities have been found in virtualization platforms in recent years, which can cause Virtual Machine (VM) escape. The frequent question is: How to avoid or prevent VM escape?

- Denial of Service Attacks

Distributed Denial of Service (DDoS) is the most common attack for cloud services. A DDoS attack floods or consumes a large amount of the bandwidth of the target system, affecting system availability, consuming large amounts of processing resources, slowing down response times, and even paralyzing the system.

The DDoS attack is a frequent visitor to data centers, wasting a great deal of administrators' Operations and Maintenance (O&M) time. Hundreds-of-Gbit/s attacks are not rare now in today's China. When attack traffic exceeds the bandwidth of a CSP data center gateway, cooperation with carriers becomes necessary. Huawei has researched and developed anti-DDoS products for more than a decade. These products are widely deployed on carrier networks and data centers around the world. Huawei leads the industry in this regard and initiated the Cloud Mitigation Alliance (CMA) to bring together carriers, Managed Security Service Providers (MSSPs), and Internet Data Centers (IDCs) across the globe to build a cloud anti-DDoS ecosystem, achieve near-source mitigation, and better handle DDoS attacks.

- Malicious Insiders

Threats may come from different types of insiders, such as current or previous employees, system administrators, contractors, or business partners. The purposes of malicious behavior may range from data theft to revenge on the company.

A remarkable difference of the public cloud from traditional networks is that the tenant data managed by public cloud administrators does not belong to CSPs. An essential goal for the public cloud design is to prevent malicious behavior of insiders. To this end, traditional administrators have limits to their authority to access, debug, and/or troubleshoot the systems they are hired to operating. A customer's system and data have to be protected from any unauthorized access. Otherwise, it is not a good public cloud design.

- Abuse of Cloud Services

The lack of VM security awareness by tenants creates vulnerabilities that will generate exposure opportunities for illegal or unauthorized access.

A CSP must also be able to monitor malicious behavior on tenants' VMs. Such monitoring should definitely avoid going too far. For example, obtaining a tenant's private information must not be allowed. Additionally, an information security system is mandatory for a public cloud deployed in China to identify content involving pornography, gambling, drug trafficking, and other illegal activities.

- Compliance Concerns

Many listed companies, government agencies, hospitals, and other customers face a series of regulatory compliance requirements outside China. Some industries in China are also restricted by such requirements as the *'Multilevel Protection Scheme.'* IT infrastructure and O&M must meet these requirements. However, when services are migrated to the cloud, customers worry that the services may fail these compliance requirements. In fact, many companies

in the industry provide compliance certification and consulting services to address customers' concerns in this regard.

Major Strategies for Cloud Security

To handle the security risks mentioned above and win customers' trust, CSPs must adopt a variety of means such as technologies, compliant operations, and information transparency. To achieve a good cloud security defense, CSPs must think like a hacker and 'understand your enemy to better defend yourself.' Vulnerabilities are omnipresent, and attack technologies are fast-growing. Defenses that rely on single methods are inadequate; therefore, a comprehensive solution is needed to build a defense-in-depth mechanism.

- General Strategies

• Build an end-to-end defense-in-depth mechanism with data.

• Realize intelligent threat awareness using such technologies as machine learning and Big Data analytics.

• Achieve automatic and visualized security O&M and compliant operations.

• Select trustworthy partners.

- Security Technology Strategy

• **Promote a Secure Development Lifecycle (SDL) with data to build security quality into design and improve security quality from the beginning:** The process of SDL is critical, but many people fail to see it. Major software companies in the industry actually regard SDL as essential. Products developed without SDL are easily exploited. Furthermore, the security of poor-quality basic software cannot be protected effectively using other defense measures. For example, high-risk vulnerabilities caused by buffer overflows have been difficult to avoid in recent years, most likely because SDL has not been deployed or is not well implemented. To mitigate the risks for APIs and UIs previously mentioned and effectively reduce vulnerabilities, good security design and programming are essential.

On October 21, 2016, many U.S. cities experienced a disruption of network services due to the DDoS attacks caused by IoT device vulnerability exploits. However, the root cause is the fact that many small IoT vendors have no secure development process and, thus, create a large number of vulnerabilities that could have been avoided. For example, some IoT devices have hard-coded default accounts with unchangeable passwords, which can only be resolved by firmware upgrades. This is a simple design mistake. Conversely, Huawei strictly implements SDL to improve security quality.

Huawei emphasizes the design of an end-to-end security architecture with data security as the core, covering all aspects such as key distribution and management, authentication, administrator account management, data encryption, and isolation of security zones. Any mistake can lead to data breaches. To better protect tenants' private data, Huawei uses encrypted search technology to ensure that even administrators cannot obtain the data.

Clouds, as large systems, require standardization of development systems to reduce vulnerabilities and dependence on experts. For example, clouds need a standardization of programming language, Operating System (OS), web framework, API framework, and virtualization platform. Cloud products are generally

> To handle the security risks and win customers' trust, CSPs must adopt a variety of means, such as technologies, compliant operations, and information transparency. >>

developed by following DevOps methods. To accelerate delivery, R&D staff needs to work on automated security testing.

- **Build defense in depth, prevent single points of penetration, and increase exploitation difficulty:** Multi-layered defense mechanisms must be established in the architecture for both products and solutions to make them hard to attack. For example, you can harden the OS using SELinux, enable Data Execution Prevention (DEP), and Address Space Layout Randomization (ASLR) to increase exploitation difficulty, protect code from being tampered with trusted computing techniques, and encrypt critical data so hackers cannot crack it. Anti-DDoS also requires multi-layered defenses, such as preventing flooding the ingresses of backbones through cooperation with carriers and creating a DDoS mitigation system within the data center. In addition to eight industry-recognized security design principles including the principle of least privilege, defense in depth is now regarded as a basic principle of security architecture design. Introducing this military concept to security architecture design is a major breakthrough.
- **Isolate to protect the security of the entire system or key zones:** Here, isolation refers to the network and software layers. Network isolation, including that for security zones, is the most basic function in a security solution. Costs, management, and other factors must be balanced; therefore, the isolation is not absolute. However, different security level zones are better isolated, as are zones for distinctive services. For example, the UI must be isolated from authentication and billing systems, which have high security requirements. Proxies are used on APIs provided to users for isolation if required.

Software isolation, such as putting an application in a container, can build a wall between the application program and other systems to minimize destructive interactions. For example, applications must be assigned with minimum privileges and no root privilege, and isolated from the OS. Isolation can also be achieved using the latest hardware technologies. For example, Intel Software Guard Extensions (SGX) technology can be used to protect critical software and data in enclaves so even if the OS or hypervisor is penetrated, the code and data in enclaves are unaffected.

- **Deploy an all-round threat awareness system on the assumption that someone has intruded into a system:** It is impossible to build a system that will never be compromised, which has been proven time and again. As long as we assume that someone will intrude into the system someday, our point of defense will change fundamentally.

“It is impossible to build a system that will never be compromised, which has been proven time and again. As long as we assume that someone will intrude into the system someday, our point of defense will change fundamentally.”

Assuming that any key zone may be broken, we have to monitor the infrastructure, platform, and applications comprehensively to avoid any blind spot. For example, we can deploy an agent on a server to output information, such as configurations, processes, and access logs, and analyze the information systematically to identify intrusions effectively. Such deployment also serves as an effective means of auditing to prevent malicious behavior of insiders and can monitor whether cloud services are abused. However, we need to obtain consent from tenants for operations involving their systems on top of VMs and make the deployment optional for tenants' use based on their needs.

To avoid VM escape, the industry mainly relies on monitoring, such as that of the hypervisor or underlying configurations. Without monitoring, attackers can do anything after they compromise the system. Monitoring is an instrument that serves a function similar to a surveillance camera or an infrared sensor in a house. Avoiding these two instruments is difficult for an intruder, unless the instruments are broken. To prevent attackers from finding countermeasures, we will not disclose these monitoring technologies to the public.

In addition to assuming that someone will intrude into the system someday, we still need to implement comprehensive enhancements to the system's security design. For example, how do we protect confidential data if the OS is compromised? First, we need to encrypt important data but cannot store the encryption key locally. This measure prevents attackers from decrypting the data even if they obtain the data. Second, we need to provide defense in depth for zones to which we believe only administrators have access. We also need to use authentication and encryption for internal machine-to-machine communications.

Cloud security solutions also need to make use of deception technologies. Gartner listed deception technology as one of the top 10 information security technologies in 2016. Deception is one of the most important active defense techniques for critical threat perception that is essential in cloud systems. The more you make the camouflage look real, the more the camouflage is able to attract the attacker to spend

more time attacking false targets. The traditional honeypot belongs in this technology category, but honeypot techniques are relatively simple and easily solved by smart attackers. The direction of focus for deception technology is to develop a variety of integrated means for the purpose of identifying the deception.

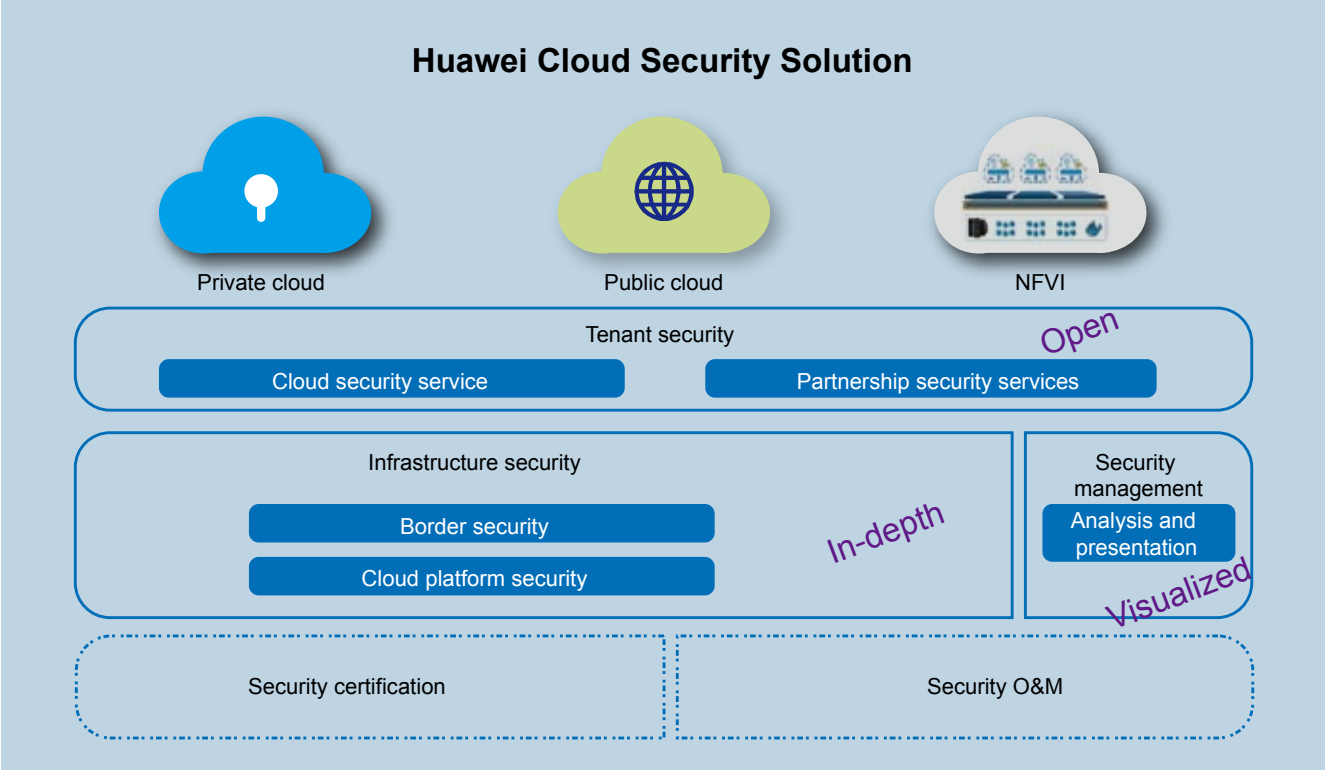
• **Deploy systems for machine learning and Big Data analytics to realize intelligent security:** The number of security logs generated by a cloud system every day is far beyond the capability of manual analysis. O&M personnel find it hard to know where real threats and attacks are. It is essential to apply systems for machine learning and Big Data analytics. Huawei has deployed a Big Data analytics platform in the public cloud in China to assist security O&M personnel in decision making and improving the security analysis capability. The platform is a critical technology of the new-generation Security Operation Center (SOC). The industry also emphasizes a combination of the SOC system and threat intelligence. The core of threat intelligence is to know yourself and your adversary well. We should not rest in reactive defense but should proactively analyze and understand attackers' latest trends, methods, tools, locations, and identities. CSPs should accumulate the capability themselves and also need to cooperate with the industry to obtain up-to-date information. Machine learning and Big Data analytics are important ways of accumulating threat intelligence.

• **Realize automatic and visualized security O&M:** Clouds have a large scale, but only a few security O&M personnel work on the clouds. We must realize automatic and visualized security O&M as much as possible. Moreover, today's clouds impose higher skillset requirements for the new generation of security O&M personnel, who should be proficient in programming so they can write scripts or develop tools to automate the work as needed.

Here are some typical examples:

1) Monitor the security status of the whole network comprehensively and realize visualized security. We should be clear about applications, OS versions, and patches of all

Clouds have a large scale, but only a few security O&M personnel work on the clouds. We must realize automatic and visualized security O&M as much as possible. >>



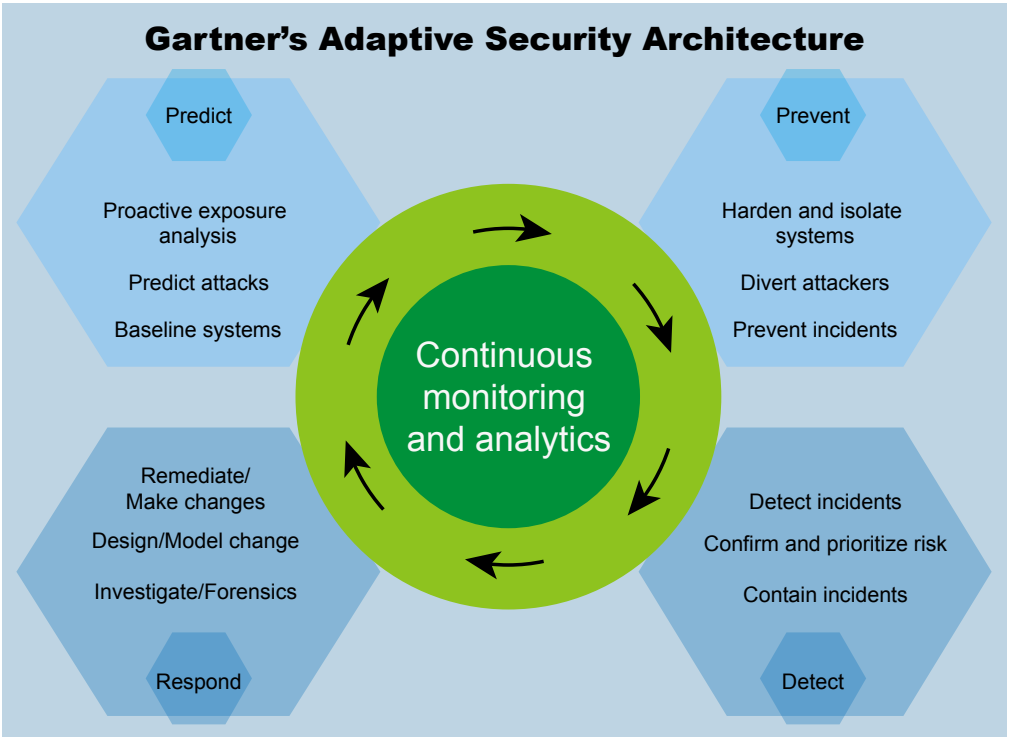
Security services in the cloud era should place continuous monitoring and analytics at the core and cover the four aspects of prediction, prevention, response, and detection. >>

components across the whole network at a glance. If a vulnerability is exposed, the monitoring system can tell us which device needs patching and can generate e-flows automatically to promote fast patching and fixing. In fact, most intrusions in the industry are not caused by zero-day vulnerabilities but by late patching of a known vulnerability.

2) Introduce online automatic security testing methods, such as real-time detection of system vulnerabilities, weak passwords, and security risks caused by incorrect configurations, so we can identify risks before the attackers do. Attackers use many tools to scan the public cloud every day and can easily find a vulnerability, if not very deep, in a public cloud. We cannot take chances and think that we are secure all the time. We should introduce the latest automatic testing tools to catch up with attacks, because the speed of attackers updating their tools is much faster than we think.

3) Realize monitoring, automatic analysis, orchestration, and delivery of security policies, which is called Software-Defined Security (SDS). For example, mistakes may occur when we modify security policies of many firewalls. In addition, security policies have to be dynamically migrated along with dynamic migration of VMs.

- **Use an adaptive security architecture:** Public clouds can be attacked at any time, with intrusion and anti-intrusion happening often. Therefore, the industry has proposed the concept of an adaptive security architecture. Security services in the cloud era should place continuous monitoring and analytics at the core and cover the four aspects of prediction, prevention, response, and detection. As an additional feature of this architecture compared with others, prediction can enhance threat intelligence and can more proactively identify and handle risks so we can take actions in advance.
- **Provide security solutions to secure tenant systems:** In principle, tenants are responsible for the security of systems on top of VMs, but many tenants lack such security capability. On one hand, we should incorporate security capabilities that are embedded within the cloud service platform. On the other hand, we can cooperate widely with security suppliers in the industry. For



example, we can broadly cooperate with industry security suppliers and integrate security products, such as DLP and intrusion detection, with our solutions for tenants to choose based on their specific needs.

- **Enhance the vulnerability management capability and speed up emergency response:** Public clouds have a large number of software programs, many of which are open source, and public cloud services are rolled out quickly in iterations. Therefore, we need to take effective measures to reduce vulnerabilities and risks.

First, we should enhance vulnerability intelligence work and consider bug bounty programs. As a CSP, we can cooperate with industry vulnerability organizations to make sure that we are aware of a vulnerability in open-source software immediately after the vulnerability is exposed; we should also build a security ecosystem so white hats in the industry can report vulnerabilities to us immediately after they find them. We can give bounties to those who report vulnerabilities proactively. This method is crowdsourced testing in nature and a win-win method.

Second, we should build fast capabilities for emergency response suitable for the Internet era. Racing with attackers is the nature of responses to public cloud emergencies. We often need to fix a high-risk vulnerability within 24 hours after exposure and need senior experts, tools, technologies, and mandatory requirements for O&M. Automatic patching tools must be in place for public clouds. Hot patching must be supported as much as possible. Hot migration should be supported to avoid service interruption caused by cold patching. The cloud OS should be consistent for O&M convenience. We can use an OS whitelist for management. We should also decouple the version release of the OS and upper-layer services so the OS and services can be patched separately.

- Compliant Operation

Compliant operation is the ground for us to win trust from others and an important way to prevent internal attacks. We need to have not only O&M management mechanisms and implementation requirements but also basic technical requirements for the cloud platform. The industry has many security certification programs that can improve our capability of compliant operation and reduce customers' concerns about compliance and data breaches. In fact, many customers base their trust on which authoritative certifications cloud services pass.

> Huawei products and cloud services have passed many international security certifications. Huawei also assists global partners in obtaining cloud security certifications. >>

As a leading ICT solutions provider worldwide, Huawei products and cloud services have passed many international security certifications. Huawei also assists global partners in obtaining cloud security certifications, such as ISO 27001, CSA STAR, and TUV Trusted Cloud.

- Information Transparency and Trust

Trust is a major issue when customers use the cloud. A CSP needs to provide sufficient information, such as the cloud infrastructure security, privacy protection, and compliance, so customers believe that the CSP is trustworthy. The provider should resolve issues proactively. For example, use a security white paper to deliver the message of cloud security. Make the information transparent, and win trust by setting up a website to provide security and privacy protection information. Publicize timely answers to security issues that customers are concerned about. Actively participate in presentations at security conferences or media promotions. Pass security certification to help build customer trust.

Huawei Cloud Security Solution

Huawei's cloud security solutions consist of tenant security, infrastructure security, and security management. Regarding tenant security, Huawei provides an open platform and works with partners to supply tenants with rich security services. Regarding infrastructure security, Huawei provides an all-stack security defense system covering networks, applications, and data to realize defense in depth. Regarding security management, Huawei has realized visualized security so risks can be presented, policies can interwork with each other, and trends can be assessed.

Huawei's cloud security solutions not only secure the enterprise cloud of Huawei but also provide solid security support for China Telecom's Tianyi Cloud, Deutsche Telekom's Open Telekom Cloud, and Telefónica's Cloud.

Vision for the Future

The only way to cope with security threats is to keep pace with the latest attack and defense technologies in the industry. For example, machine learning and Big Data analytics are promising security technologies, and we should also pay attention to automatic machine attacking and defense. Further, we should enhance cooperation on threat intelligence within the industry to improve our security defense capability through joint efforts. ▲

Historic Mission and Key Tasks for CIOs in the Digital Era

By *Yan Lida*

A new generation of information technologies, such as the Internet of Things (IoT), Cloud Computing, Big Data, and Artificial Intelligence (AI), are profoundly redefining various industries with unprecedented depth, scope, and pace. The primary sector (agriculture) will see the greatest leap in production efficiency since the industrial revolution, as information, automation, and intelligence not only enhance production capacity and quality but also free people from mundane labor to focus on more intellectual areas. Smart manufacturing enabled by innovative Information and Communications Technology (ICT) is rapidly reshaping the entire secondary sector (industrial businesses), and emerging virtual enterprises that are built on new ICT platforms are opening a new chapter in the history of manufacturing. The revolution of the tertiary industry (services) is expected to be the most exciting, with continuous emergence of people-centric service innovations. For instance, in the past a bank was merely a place for financial transactions, while future banking will be based on a set of 'behaviors' instead of being a geographical location. The core element of urban development in the past was 'governance,' while that of a new Smart City will be people-oriented services. In the past, the creation of media has centered on the producer, while media nowadays focuses on the 'prosumer' (a consumer who is a producer). In the digital era, the increasing complexity of the world prompts us to think about the basic features of future enterprises, and the mission and tasks that will be undertaken by their CIOs.

Yan Lida

In the digital era, enterprises must implement digital transformation and evolve towards a digital enterprise with unswerving commitment. At the same time, Chief Information Officers (CIOs) have to take on a historic mission, evolving into CI^{3}Os and leading the digital transformation of enterprises.

Three Basic Features of Future Enterprises

To succeed, enterprises need the right features to be able to adapt to meet the challenges and opportunities of a new era. Looking deep behind the scenes, we can summarize the three core features of future enterprises as follows:

- IT-Enablement — Enterprises in the 21st Century are Primarily 'IT Enterprises'

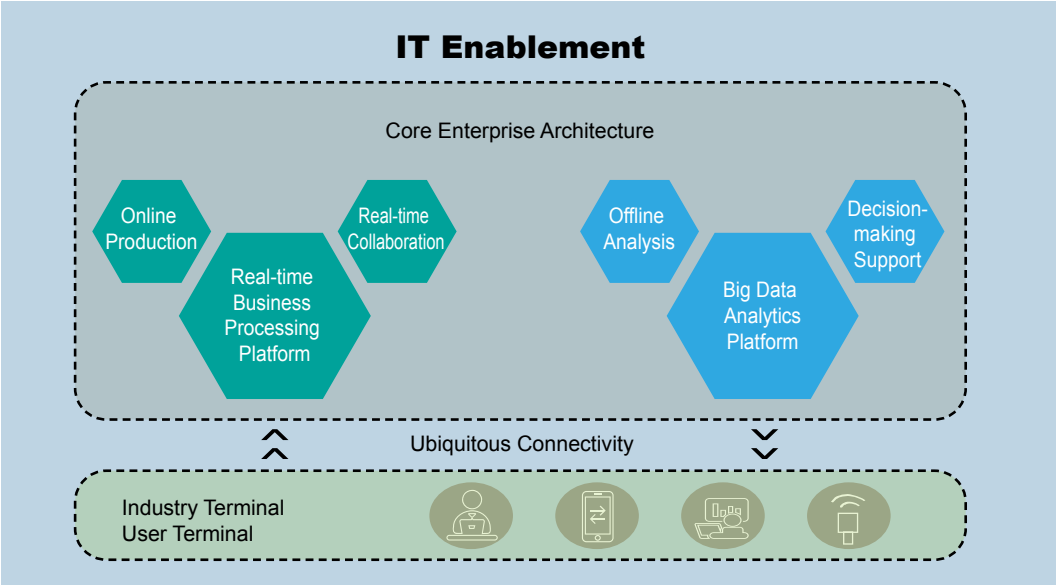
In the digital era, every company is first and foremost a digital enterprise. Since IT systems act as production systems for enterprises in the Internet, telecommunications, and finance industries, the performance of IT systems directly determines enterprise productivity. For traditional enterprises, the application of digital technologies will be one of their core competitive advantages in the future. The new generation of information technologies not only facilitates automated office and business processes as well as smart knowledge management but also penetrates deep into the manufacturing system and the ways products and services are used. This is reflected in three aspects. First, ubiquitous connectivity links people, things, businesses, and knowledge together, rendering everything digital. Second, cloud computing converts mass digital data into resources to support businesses. Third, Big Data enables companies to transform resources into profitability. In the future, the IT architectures of enterprises will undoubtedly transform from the traditional 'siloed deployment' to the model of 'Real-time Business Processing Platform + Big Data Analytics Platform + Industry Terminal.' IT is coming forward from behind the curtains to promote the automation and intelligence of enterprises, and will be at the heart of future enterprises.

- Innovation-Driven — Innovation is the Essential Rule of Business Survival When the Economy is Moving from Scarcity to Surplus

In the digital era, enterprises will continuously strive for innovations in business models and operational systems to improve business efficiency and the user experience. Novel approaches that are led by customers, driven by data, and enabled by enterprises and employees in real time have brought tremendous changes to enterprises, which can be dealt with, managed, and embraced by enterprises only on the basis of constant innovation. Such innovation consists of both internal innovation in processes, working methods, operating systems, and business models, as well as joint innovation with customers and partners. Enterprises should create platforms to support comprehensive innovation, because this is the only way to get close to their customers, and to be efficient, agile, and dynamic. Innovation will be a vital feature of future enterprises, as the DNA of innovation is necessary for all industries.

- Ecosystem Construction — Fighting Alone is Outdated, and Enterprises Prosper Only in a Thriving Ecosystem

As enterprises undergo digital transformation, the vision and strength of a single enterprise cannot by itself address all the changes in the outside world. The previous competition between enterprises is now equivalent to the competition between ecosystems. In addition to products, services, and business models, an enterprise's competitive advantages will include its positioning in the ecosystem and relationships with partners, as well as its ability to integrate and utilize external resources. In this context, enterprises need to offer



> IT is coming forward from behind the curtains to promote the automation and intelligence of enterprises, and will be at the heart of future enterprises. >>

their capabilities as modules and services, and build open platforms, which will help them achieve agile operations and encourage efficient collaboration within the industry chain. Moreover, enterprises are expected to accomplish resource sharing, cross-border innovation, and symbiotic development with customers, partners, and members of the industry ecosystem. By doing so, the disruptive power of enterprises will be unleashed to deliver a new value experience for customers. Therefore, enterprises, especially the large ones, will become ecosystem builders. The ecosystem will be at the heart of future enterprises, and businesses will prosper only in a thriving ecosystem.

CIOs' Historic Mission in the Digital Era

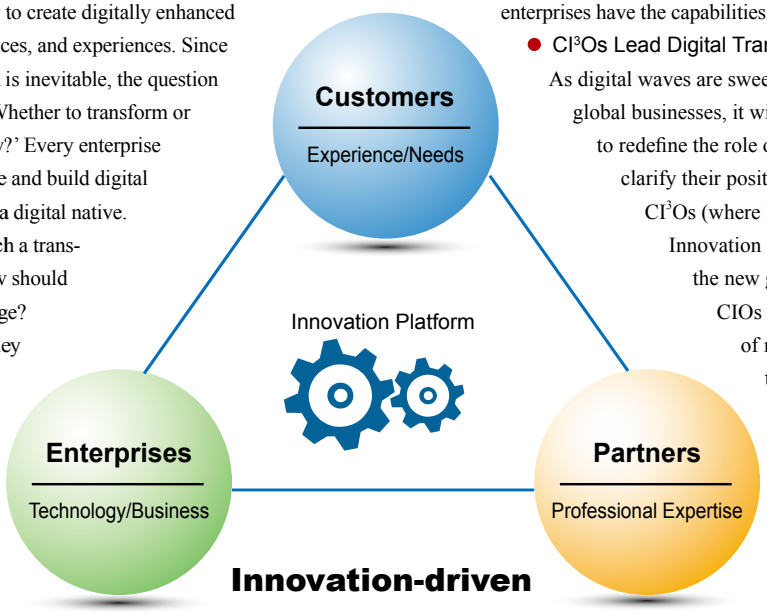
All departments within an enterprise are moving towards the digital economy. International Data Corporation (IDC) predicts that, by 2020, 50 percent of the Forbes Global 2000 will see the majority of their business depend on their ability to create digitally enhanced products, services, and experiences. Since transformation is inevitable, the question is no longer 'Whether to transform or not?' but 'How?' Every enterprise has to conceive and build digital platforms like a digital native. Faced with such a transformation, how should the CIOs change? How should they position themselves? And what will be their historic mission?

● Traditional CIOs Face Enormous Challenges in Times of Rapid Change

Technologies previously progressed step by step, but now they are making enormous strides forward. The cycle of technology regeneration is getting shorter and shorter with continuous upgrading, and CIOs and IT staff need to navigate these ongoing changes. After building traditional IT architectures, more CIOs and IT staff are now becoming 'creators' of digital platforms, which enable innovations in enterprise strategies, business processes, organizational structures, and ecosystems. This creates new challenges for CIOs. Driving forces such as the IoT, cloud computing, Big Data, AI, and security must be coordinated, and CIOs must keep pace with the times and seize the trend. For example, in the future multi-cloud era (consisting of a universal public cloud, and an enterprise private or hybrid cloud), CIOs must be able to build and use the cloud to achieve digital transformation. However, how many CIOs in traditional enterprises have the capabilities to achieve this?

● CI³Os Lead Digital Transformation

As digital waves are sweeping across global businesses, it will be important to redefine the role of CIOs and re-clarify their position and mission. CI³Os (where I³ = Information + Innovation + Interconnection), the new generation of CIOs will be the leaders of new information technologies, the drivers of enterprise innovation, and the enablers of ecosystems.



Driving forces such as the IoT, cloud computing, Big Data, AI, and security must be coordinated, and CIOs must keep pace with the times and seize the trend. >>

- Leaders of New Information Technologies (Information)

Enterprise digital transformation will be a top-level movement based on new IT architecture that will be created by CI^{3}Os. A CI^{3}O holds a key role in an enterprise's adoption of new technologies and ideas, with easy access to new technologies like cloud, Big Data and AI, and pioneering thoughts behind them. Enterprises need CI^{3}Os who have an outstanding technological vision and business acumen, as well as the ability to lead digital transformation and innovation teams to seize new opportunities and accelerate technical monetization. CI^{3}Os will become the leaders in new information technologies.

- Drivers of Enterprise Innovation (Innovation)

In the digital era, CI^{3}Os are both the technological leaders and innovation drivers of their enterprises. With a comprehensive understanding of business development strategies, they need to focus on building innovative enterprise platforms by using new technologies and approaches such as interactive experiences, knowledge sharing, and digital flow to boost the all-round innovation in operating systems, business models, and user experiences. Consequently, they will manage to reduce the operating costs and create new business value for the enterprise. CI^{3}Os are becoming the drivers of enterprise innovation.

- Ecosystem Enablers (Interconnection)

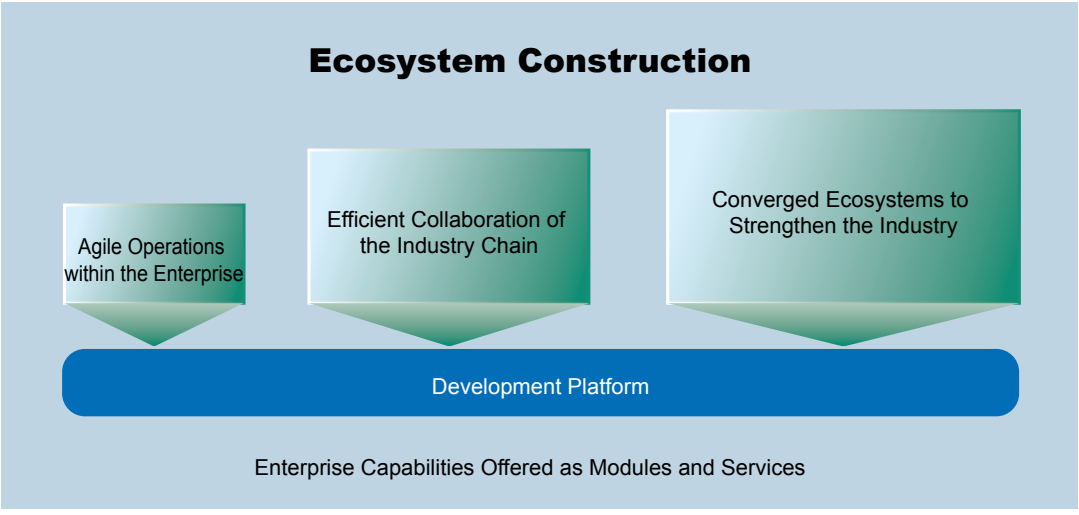
Enterprises should build a digital business ecosystem that integrates customers, partners, and employees. Such an ecosystem is open, dynamic, and diversified, and supports interactions with customers, partners, associated industries, and even competitors. By building open platforms, CI^{3}Os can open up and share the enterprises' capabilities, and create an ecosystem with positive interactions to support the integration of internal and particularly external resources of the enterprises. The way different organizations interact in the digital world will transform traditional businesses in a linear value supply chain into the new businesses in a networked digital ecosystem, with CI^{3}Os assuming the role of the enabler. Therefore, CIOs no longer play a supporting role but more of a leading and a strategic one. In this new era, CIOs need to drive innovations in enterprise strategies, business processes, ecosystem models, service models, and products through information technologies.

CIOs' Key Tasks in Evolving into CI^{3}Os

Digital transformation cannot be completed overnight in any industry, whether in terms of management, organization, or individuals. In the face of such a historic opportunity, let us take a look at the changes in various industries and outline the evolution from CIOs to CI^{3}Os.

- CI^{3}Os Must Build New ICT Architecture to Address Pain Points and Deliver New ICT Layouts in Line with the Enterprise's Business Strategies

To create a digital enterprise, in various business scenarios, ubiquitous connectivity must be implemented between people and people, people and things, and things and things, as



CIOs no longer play a supporting role but more of a leading and a strategic one. In this new era, CIOs need to drive innovations in enterprise through information technologies. >>

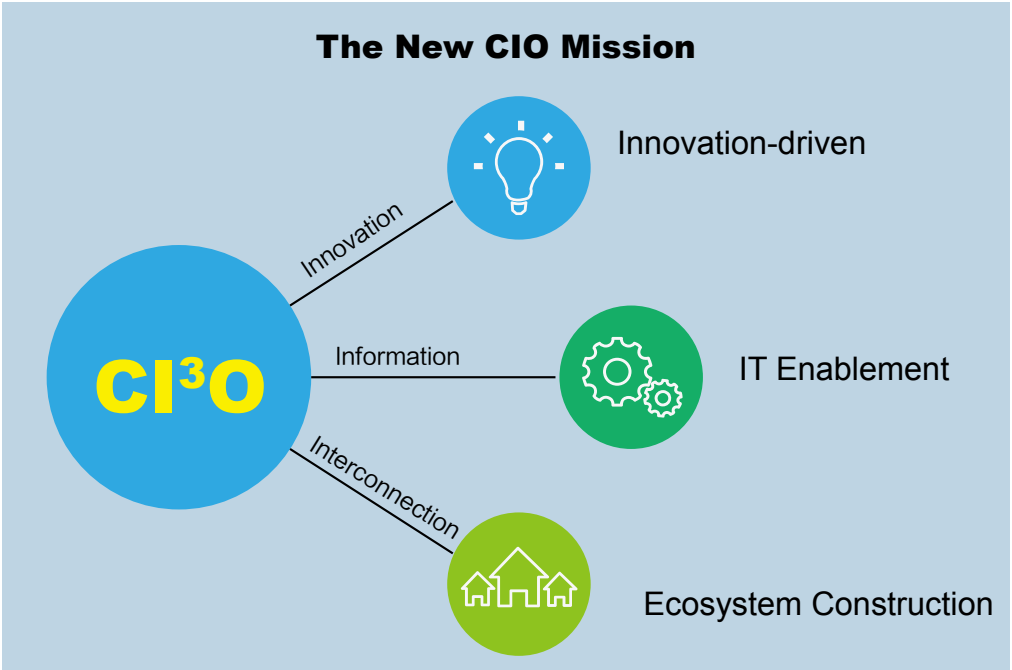
well as among employees, customers, partners, and suppliers. Real-time decision making should be integrated into business processes to power automation that makes operations simpler, smarter, and more efficient. The essence of a digital enterprise is to provide customers, partners, and employees with the ROADS experience — Real time, On demand, All online, DIY, and Social — in buying and using the products and services, both from the perspectives of enterprises and the consumers. In terms of business volume, Gartner forecasts that, by 2020, over 26 billion devices will be interconnected to generate 215 trillion stable connections and 63 million transient connections every second, generating massive amounts of data. Meanwhile, since the need for real-time analysis goes far beyond traditional analysis, there will be a huge number of concurrent calculations. Conventional IT architecture is unable to meet such massive demands. For this reason, the CI^{3}O needs to build a new ICT architecture platform that is powered by the IoT, cloud computing, Big Data, and AI, and supported by augmented reality, virtual reality, and new security technologies to set up a new ICT layout in line with the enterprise's business strategies.

● CI^{3}Os Must Adopt New ICT to Drive Innovation in Business Models, Operating Systems, Products, and Processes

As a leader in building an enterprise's digital platform, the CI^{3}O must integrate new ICT into businesses to accelerate innovation, revolution, and remodeling, as well as improve the experience and efficiency of traditional businesses.

For example, in the finance industry, a Chinese online bank has reached 450 million users — the number of users of China's largest established bank — in just five years. Its operational indicators are much better than those of conventional banks, with its loan cost of less than USD 0.291 (CNY 2.00) per transaction versus USD 291 (CNY 2,000) per transaction for conventional banks, and a capital loss rate of 0.001 percent versus one percent for conventional banks.

In the manufacturing industry, CI^{3}Os need to utilize new ICT platforms to build the core capabilities of smart manufacturing — AI^3. These comprise 'R&D Integration' in the entire product lifecycle; 'Horizontal Integration' in the demand and supply chain ecosystems; 'Vertical Integration' from the business system



to the operating system; and 'Smart and Automated Production.' Smart manufacturing can help innovate products, operating systems, and business models. For instance, the aircraft engines sold by manufacturers only account for 30 percent of the value created in the entire product lifecycle, while engine maintenance and repair services account for 70 percent of the total revenue. In the field of elevators, various types of sensors in an elevator can transmit its operating conditions to the Operations and Maintenance (O&M) center in real time to deliver predicative maintenance and fast fault recovery, creating a new sales model based on elevator usability.

In the field of traditional media communications, the producer is at the center of one-way communication, which features single-channel sources, closed production, and point-to-mass transmission. With the rapid spread of smart terminals and high-definition video broadcast, everyone is able to discover and release content at any time, which has changed the workflows and mechanisms of media communications. CI^{3}Os need to build a platform for digital production of convergent media to enable complete sharing of content and simultaneous distribution of one-time-developed content to multiple channels, including television, the Internet, and mobile phones. The platform also needs to ensure the timeliness, accuracy, and coverage of media communications.

- CI^{3}Os Must Propel the Restructuring of Enterprise Organizations and Processes to Enable Digital Operations

In the future, an enterprise will be first and foremost a digital enterprise, and its performance will be measured by a set of strict digital standards. There will be an inevitable trend for enterprises to adopt digital operations to improve their efficiency in the supply chain, product management, interest chain interaction, and knowledge transfer, and to ensure a high-quality customer service experience. As the focus of digital operations, digital businesses will need to drive new processes and achieve new targets and results. The CI^{3}O has to determine how to support digital operations by using new technologies, such as mobility, micro service, Big Data, and AI, to redesign business processes and empower the organization.

A number of global virtual enterprises will emerge that break down the tangible boundaries of traditional enterprise organizations, and operate based on the new ICT architecture. >>

The CI^{3}O should redesign business processes based on new technologies, not only for the sake of using new technologies, but to drive real-time, online, transparent, and intelligent processes. For instance, the online financial services have adopted new ICT to transform the traditional banking processes, which previously had fixed steps including 'application, review, and granting,' into new procedures comprising 'review upon activation, on-demand application, and real-time granting,' shortening the one-week loan granting cycle to less than a minute.

In terms of organizational structure, throughout the progress of digital operations, the CI^{3}O needs to build a product operations team that is closely integrated with business departments, integrate product operations, and raise the status of the IT team. For example, leading mining companies have integrated IT and Operating Technologies (OT) departments to form a new 'Production System Operations Department.' A large bank in China has built an 'information-based bank' and elevated the status of its IT departments (Guangzhou Development Center, Shanghai Data Center, and Beijing Data Center) from their previous supporting roles to departments directly reporting to the Head Office.

It can be expected that, with the deepening of digital operations, a number of global virtual enterprises will emerge that break down the tangible boundaries of traditional enterprise organizations, and operate based on the new ICT architecture. These virtual enterprises will manage to integrate global resources via the IT platforms, and deliver production capacity more quickly than the conventional models, greatly reducing the time required in product design, manufacturing, processing, and maintenance. In addition, more intelligent product operations and business models are facilitated by the digital platforms to advance the business history of mankind to a new stage.

As CIOs of enterprises become aware that IT is a strategic asset, they also must understand the importance of the role of CI^{3}Os, who are best-placed to lead their companies' digital transformation. The ability to accomplish industrial upgrades with IT is a critical point on the way to implementing the strategic purpose of each enterprise. Only in this way will companies come to be truly digital enterprises with strong ecosystems that help drive innovation. ▲

ICT INSIGHTS 【 Extra 】

Contributions and Feedback

To be an informative and inspiring magazine, *ICT Insights* needs your continual contributions and feedback. Please feel free to submit articles for publication. The editors greatly value your input.

Contact us by email: ICT@huawei.com
Call us: +86 (010) 82882758

We look forward to hearing from you.

Facebook Twitter Linkedin Youtube