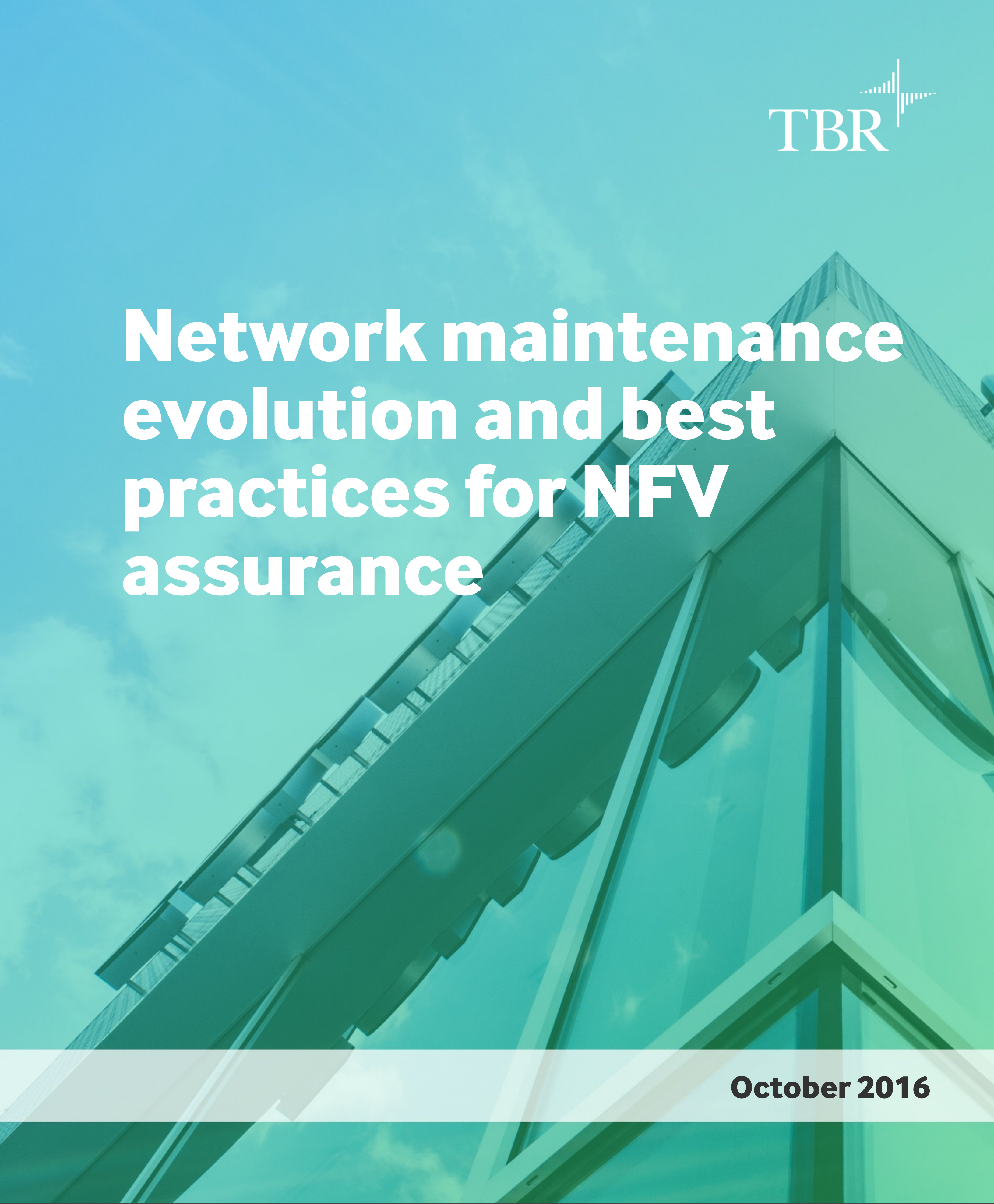


TBR

Network maintenance evolution and best practices for NFV assurance

October 2016

TECHNOLOGY BUSINESS RESEARCH, INC.

CONTENTS

Introduction: NFV transformation drives new network assurance strategies

Telecom service providers testify they are responding to pressures on their business models by changing the way in which they design, develop and deliver services. This transformation is targeting a shift from today's legacy network operations to implementing a transparent service delivery, operations and management environment that enables customers to self-service and monitor service-level agreements (SLAs) and key performance indicators (KPIs). A key goal is to give customers the capability to activate changes and upscale, downscale or alter services on demand. This is an urgent need because operators are challenged to differentiate to increase revenue in the face of slower growth and greater competition.

Most operators see NFV and cloud platforms as the means to enable their transformation. NFV offers the promise of decoupling services from physical single-stack systems to distributed virtual functions or service chains that are automated, controlled and orchestrated from a common platform.

> "We are overcoming dependency on hardware upgrade cycles that made the services inflexible, and replacing the proprietary hardware with commodity hardware and software stacks. This enables more robust services performance and flexibility than dedicated hardware-based services. But it creates concerns about recovering the service in the new software-mediated environment."
>
> — Tier 1 Operations Manager

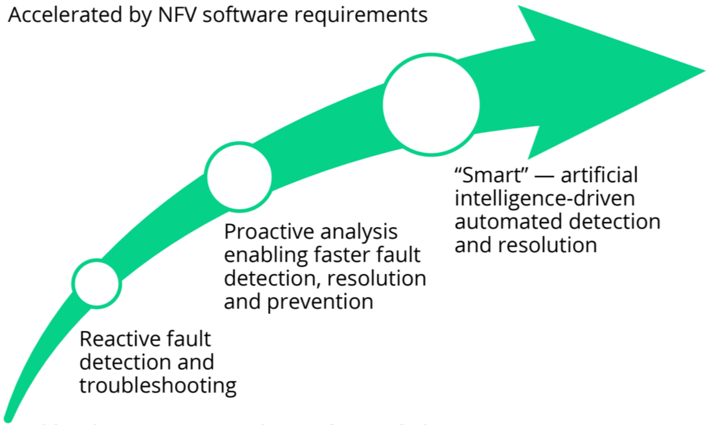
According to operators, NFV transformation requires both a change in the network infrastructure as well as a parallel shift in the way in which networks are managed to ensure redundancy and reliability. This transformation impacts existing and legacy workflows, including network assurance.

Network maintenance evolution

NFV represents a marked shift in telecom service provider maintenance workflows that have been in place for several years. In legacy networks, reliability, redundancy and recoverability were managed in a reactive manner focused on fault detection and troubleshooting. The ability to investigate and correlate faults across alarms for multiple equipment domains, followed by a fast resolution process involving a truck roll or software update, was prized.

Network maintenance evolution

Accelerated by NFV software requirements


"Smart" — artificial intelligence-driven automated detection and resolution
Proactive analysis enabling faster fault detection, resolution and prevention
Reactive fault detection and troubleshooting

SOURCE: TBR INTERVIEWS WITH OPERATORS

Over the years, operators introduced more proactive tools, applying analysis of customer and network data to determine potential network performance issues, which enabled faster detection and resolution of faults, often before the customer became aware of them. The next stage in network management is automating the detection and correction of issues through the application of “smart” or artificial intelligence technologies. These solutions provide automated responses where the network components react to policy-based thresholds, enabling greater complexity in the network and decreased operations intervention. This is not sustainable because the response time for non-automated services will be too slow to prevent service degradation.

Operator NFV Maintenance Concerns

- Dependency on hardware upgrades
- Visibility into all layers of NFV
- Network recovery delays in virtual platforms
- Assuring reliability of open-source platforms
- Lack of tools to use for software troubleshooting

SOURCE: TBR INTERVIEWS WITH OPERATORS

The evolution from passive to proactive and then to smart maintenance was underway before NFV, but it is becoming crucial as NFV introduces complexity and the need for visibility as multiple instances are running on single platforms. The cost of failure is great. NFV will accelerate the movement from monitoring to real-time intelligence and analytics that respond to preset policies to enact orchestrated alterations in the network to support service delivery.

Operator challenges and pain points

Chief among the challenges is the requirement to develop a new approach to network recovery. For example, many real-time services have recovery times of 20 milliseconds or less. With physical infrastructure, providers have been able to co-locate systems and implement redundant control and transport complexes that support the real-time services requirements. But with NFV, the risk of failing to recover in the required time is greater as the same distributed architecture that makes services transparent and flexible also enables services to be executed across diverse hardware and software platforms that can be located anywhere in the network.

Service execution will also depend on multiple software functions or control systems, increasing the possibility of disconnected process steps. This issue is one of the causes of conflict within service providers about NFV implementation.

Another concern is the state of the existing network. Operators require help in assessing the readiness of network systems to implement NFV. System health checks — long a vital part of network maintenance — must now have an NFV lens to assess the readiness for the complexity of software-mediated processes.

> “It can take too much time to stand up network infrastructure components for the service, causing response time to slip, degrading the service and causing a reduction in service-level performance. The services can be dependent on hardware and software instances executed anywhere at any data center at any time. We are gaining savings on hardware simplification but at the cost of recoverability.”
>
> — Tier 1 Operations Manager

Added to this issue is managing the compatibility of different NFV solutions as they are implemented. Different versions of open source, as well as supplier NFV solutions, require compatibility management at a new level. Incompatible systems elements or software versions can cause further network faults.

Despite the issues, TBR's NFV research shows service providers maintain high expectations of software-mediated networks, with most providers planning NFV-based network adoption within the next two years. However, there are few solutions to prepare for the changes NFV will bring to the vital requirement of network assurance. Operators indicate that more than cloud tools will be required — suppliers will need new tools that adapt the requirements of NFV to the expectations of reliability and performance of telecom networks.

In the software-mediated network, performance will be affected in many ways. Instead of physical links connecting and marking location and, therefore, a place to apply assurance methods such as monitoring and troubleshooting, virtual interfaces will connect functions within software in different servers located anywhere.

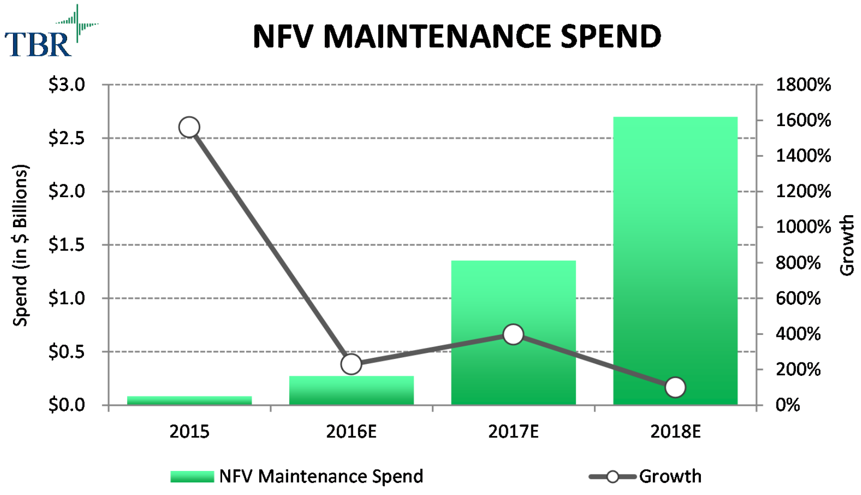
NFV Maintenance Challenges

- Adapting process methods and procedures for hybrid, physical and virtual systems
- Deepening models for proactive network assurance
- Developing new SLAs that feature real-time, contextual and location-aware assurance methods
- Creating traffic visibility between and within physical and virtual networks
- Requiring new levels of application and service awareness to detect service chain issues
- Navigating a more complex multivendor environment of heterogeneous software functions and hardware

SOURCE: TBR INTERVIEWS WITH OPERATORS

Dedicated attention to network assurance will be required for transformation to open-source platforms, commodity white boxes and instant virtual network functions.

Figure 1



SOURCE: TBR ESTIMATES

Service providers will need to budget for new investments in network maintenance to accommodate NFV. As shown in Figure 1, TBR estimates over $2.5 billion will be spent on maintenance for NFV solutions by 2018, with the bulk of the spend coming as service providers scale their software-mediated network implementations. Besides virtual probes, the spending will encompass service catalogs, orchestration environments and dedicated tools as well as vendor-supplier services to transform and enable the new NFV maintenance environment.

TBR's research indicates service providers are currently placing technical support for NFV at a low priority, despite the issues and expected investment required. While this is a cause for concern, this attitude may change between now and 2018. However, there will be no instant transformation of network assurance and there is a danger service providers will apply old solutions to new problems, causing significant growing pains in implementing NFV operations.

Progressive service providers understand the urgency of developing a game plan for NFV assurance and are beginning to identify tools and partners to help them. Many Tier 1s are also realizing they cannot invent all the methods and tools themselves, which will create an opportunity for their traditional and new support partners.

Best practice solutions

Operators state an end-to-end approach is needed where the network and service processes are viewed across domains and layers rather than on the isolated hierarchies of present systems. The end-to-end procedure has the following attributes:

- Approach the problem with a recover-first, resolve-next solution

  In the physical network, when a faulty network element was detected, the goal would be to immediately assess the root cause, which led to a significant investment in root cause analysis (RCA) tools and intelligence. This process will be shifted in NFV with the immediate recovery of the function enabled by easily replaced virtual machines (VMs) or compute/storage units. The service will be instantly recovered through isolation of the faulty unit and transfer of the workload to another VM or server. After the recovery, analysis will be conducted to determine the cause of the fault and the repair implemented.

- Apply a method for predicting potential faults and implement a plan to optimize

  While predictive tools have been deployed into the network in recent years, NFV requires an upgrade in capability. With the rapid change and increased sources of failure, in addition to the variability in location for any given function at any time, the VMs in the network must be monitored every few seconds to guarantee KPI thresholds are maintained. This service links to the previous attribute where the recover-first, resolve-next method can be applied to any VMs below the KPI threshold.

  Predictive fault detection can also be extended to the CPU or memory of the servers, which can be monitored to detect grey failures (i.e., signs of overutilization that have not yet affected performance). Overall, these methods need to be part of a multilayer fault locator platform that can detect and report faults pointing to the VM, CPU or other factors.

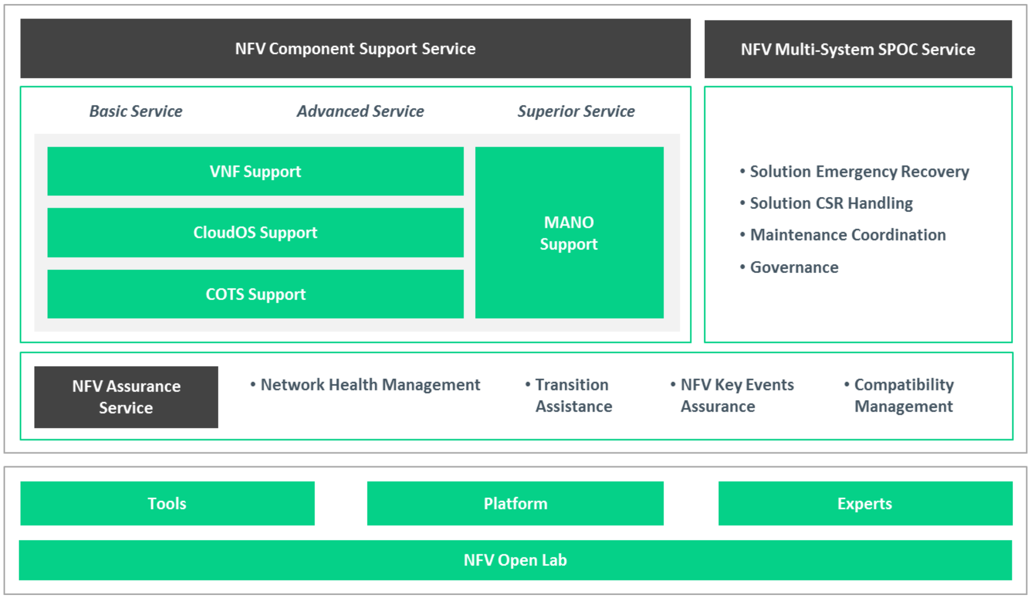
- Implement ongoing support services

  There are many additional services that can enhance network assurance processes or be part of customer support agreements with vendors. These include designating a supplier as a single point of contact (SPOC) to address the complexity of the multivendor environment, obtaining assistance for the transition from physical to virtual assurance systems, obtaining assessment assistance for NFV implementations, and leveraging supplier or third-party labs to replicate and analyze performance issues.

One example of a solution is Huawei's new services and tools for NFV customer support. As shown in Figure 2, Huawei's NFV Solution Support Services is a combination of organic additions to existing platforms for network assurance, operations and optimization, and next-generation assurance capabilities.

Figure 2

NFV Solution Support Services



SOURCE: TBR AND HUAWEI

Multivendor support has long been in place in telecom service providers, but the complexity of an infrastructure with multiple vendors participating in the service chain for a given application greatly increases the difficulties of coordinating network assurance programs. Huawei's NFV Multi-System SPOC Service addresses this issue by providing the central point for coordination across the operator's network. The large number of components within the NFV infrastructure creates unique challenges when it comes to the service provider guaranteeing a robust network, which remains a key requirement of SLAs with enterprises and subscriber contracts with end users. One way to assure the network is robust despite its virtual nature is to apply a proactive assessment process for each component.

Huawei helps service providers take a proactive approach to NFV assurance through its new Robust Network Service assessment framework and services solution. Robust Network is a scalable assessment service applicable to NFV implementations. Huawei assesses the state of the network by collecting and analyzing data in a central repository, checking the performance of key functions, and monitoring it for best practices operations and carrier-grade functions. Huawei carries out a performance audit to assess system reliability; network protection; and the health of the hardware, cloud OS, management and orchestration; and virtualized network functions (VNFs). Huawei can then design and implement solutions to improve network health, and follow that process with rigorous testing and reassessment.

This assessment can even be implemented with respect to the VMs operating within the infrastructure. For example, Huawei leverages a KPI-based recovery tool to monitor and detect deterioration in VMs. When the tool recognizes a VM performing below the KPI threshold, it isolates the faulty VM for later troubleshooting.

Taking assessment a step further, Huawei also provides tools to evaluate grey failures. As a predictive issue, grey failures are less well known to many operators. Huawei discovered two kinds of grey failures:

degrading CPU performance and overtaxed memory. These failures are detected by implementing real-time monitoring and comparing the results over time through statistical analysis. When the comparison reveals large gaps, a warning is triggered and the issue is investigated further.

NFV support also requires multilayer or cross-layer fault location, which detects faults across the NFV environment, specifically whether a fault is within the commercial off-the-shelf hardware, the NFV infrastructure or VNFs. Previously, fault detection was implemented independently for each layer. Huawei evolved the fault locator to collect data from all layers of the network for cross-layer fault demarcation and RCA.

As NFV is a relatively new technology, operator staff could be unfamiliar with best practices for dealing with issues that may arise and may require retraining to become systems engineers. With its Transition Assistance service that builds off its incumbency in traditional network managed services and applies that experience to NFV, Huawei will support a service provider's operations for the first three months or more following initial NFV deployment. In these situations, Huawei deploys its staff on-site or remotely to operate the NFV implementation, provide technical assistance and engage in knowledge transfers.

Huawei's NFV Solution Support Services includes access to its NFV Open Lab in Xi'an, China, which offers interoperable testing equipment, enabling Huawei to build an industry ecosystem for NFV. NFV Solution Support Services customers can use this resource to simulate problems occurring in the network, enabling customers to conduct interoperability testing, solution verification and software upgrade testing. The lab also provides an opportunity for compatibility management through testing of simulated infrastructure and multivendor environments.

Conclusion

Service transparency and flexibility are key to increasing customer value and remaining competitive in the eyes of most telecom service providers. NFV transformation is seen as the path to achieving these goals. NFV also represents new challenges for maintenance, specifically network assurance. Early adopter operators report top issues include recovery, training, software certification and application flow visibility. Operators are beginning to identify and address these issues. At the same time, NFV transformation will accelerate the evolution of maintenance services as the techniques of proactive, real-time analytics will support the orchestration and automation needed to tackle NFV assurance challenges. TBR expects the combination of these factors will yield $2.5 billion in NFV-related maintenance spending by 2018.

Among the investments will be new tools that address key NFV challenges with solutions such as a recover-first, resolve-next method; increased predictive fault assessment; network component optimization; single point of contact across multivendor solutions; and leveraging supplier labs and transition experience. Huawei is offering a suite of solutions for NFV assurance integrated within its existing portfolio. TBR believes these solutions hold promise to help address the crucial network assurance challenges service providers face with NFV transformation.

About Huawei

As a leading global information and communications technology (ICT) solutions provider, Huawei is innovating to provide new tools and services for NFV customer support. Huawei understands the need for next-generation network assurance brought about by NFV. Huawei is addressing this issue through services such as SPOC, transition assistance and robust network, as well as tools including its KPI-based recovery tool, grey failure detection, unified monitoring, fault locator and NFV Open Lab.

About TBR

Technology Business Research, Inc. is a leading independent technology market research and consulting firm specializing in the business and financial analyses of hardware, software, professional services, telecom and enterprise network vendors, and operators.

Serving a global clientele, TBR provides timely and actionable market research and business intelligence in formats that are tailored to clients' needs. Our analysts are available to further address client-specific issues or information needs on an inquiry or proprietary consulting basis.

For more information

TBR has been empowering corporate decision makers since 1996.
For more information, visit www.tbri.com.

This report is based on information made available to the public by the vendor and other public sources. No representation is made that this information is accurate or complete. Technology Business Research will not be held liable or responsible for any decisions that are made based on this information. The information contained in this report and all other TBR products is not and should not be construed to be investment advice. TBR does not make any recommendations or provide any advice regarding the value, purchase, sale or retention of securities. This report is copyright-protected and supplied for the sole use of the recipient. ©Contact Technology Business Research, Inc. for permission to reproduce.