Publication date:
December 2020
Author:
Adaora Okeleke

Driving Effective Telco Network Automation

Taking an End-to-End Approach to Achieving Network Automation

In partnership with:

IBM

Brought to you by Informa Tech

Contents

Summary

As communications service providers (CSPs) evolve toward cloud-native networks, they are demanding a unified platform that can deliver consistent operations across physical network functions (PNFs), virtualized network functions (VNFs), and containerized cloud-native network functions (CNFs). Automating the end-to-end lifecycle management of network functions and services in this hybrid environment is vital to simplifying operations, supporting traffic growth, and growing revenues.

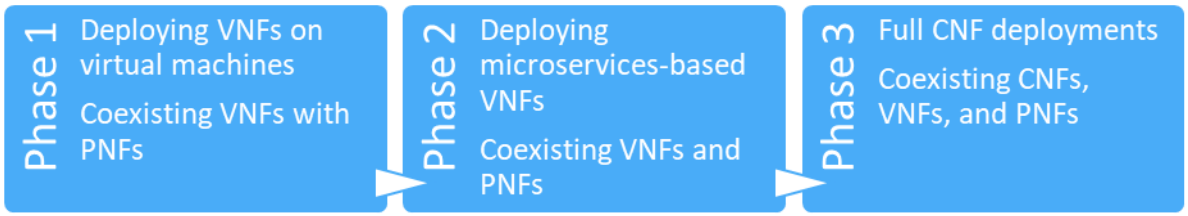
Automation is not new to CSPs. However, the scale of network complexity makes current automation strategies insufficient to achieve the end-to-end service and network management of CSPs' hybrid network environments. CSPs will need to take a more holistic approach to automation, including automating operations at the cloud infrastructure (or networking functions virtualization infrastructure [NFVI]) layer, network resource layer, and service management layer, as well as integrations across these layers. Taking an intelligence-driven approach to support this end-to-end network automation strategy becomes critical to achieving the agility, flexibility, and operational efficiencies expected from network transformation projects.

Having the right tools and technologies is not enough. While technologies such as intent-based automation (IBA), big data, and artificial intelligence (AI) are relevant, building the required skills, re-aligning processes, and transforming organizational culture are just as important to enable network automation. Adopting cloud computing operational practices such as DevOps and site reliability engineering (SRE) and implementing standard and open APIs should be key priorities for CSPs to gain the benefits of automation.

Network transformation unveils more complexity

Key industry trends around 5G, edge computing, the Internet of Things (IoT), and webscale disruption continue to drive network transformation through software-based technologies such as network functions virtualization (NFV) and software-defined networking (SDN). The key drivers include gaining increased flexibility, agility, and cost reduction when creating and managing new services and networks. NFV implementation will continue to pick up pace, and Omdia forecasts NFV revenues to reach $45 billion in 2025, growing at a CAGR of 17.2%. However, CSPs' transition from physical to virtual network environments (as shown in **Figure 1**) has created more complexity regarding network management and operations.

Figure 1: The three phases of network evolution



Source: Omdia

In Phase 1, initial VNF deployments were not cloud-native, so did not allow CSPs to reach the scalability necessary for anticipated increases in network traffic. CSPs also faced challenges such as long lead times for VNF onboarding and vendor lock-in, defeating the purpose of NFV.

CSPs and their vendors have been striving to make their deployments and solutions more cloud-native. Phase 2 (where most CSPs are today) involves re-architecting available VNFs into microservices, rather than building solutions from scratch as microservices-based functions running in containers. While this approach has made it easier to host current VNFs in multicloud environments, it has not made them as flexible or scalable as operators require. In addition, as these VNF deployments continue to coexist with PNFs, and have CNFs deployed alongside them, the complexity of managing these environments increases.

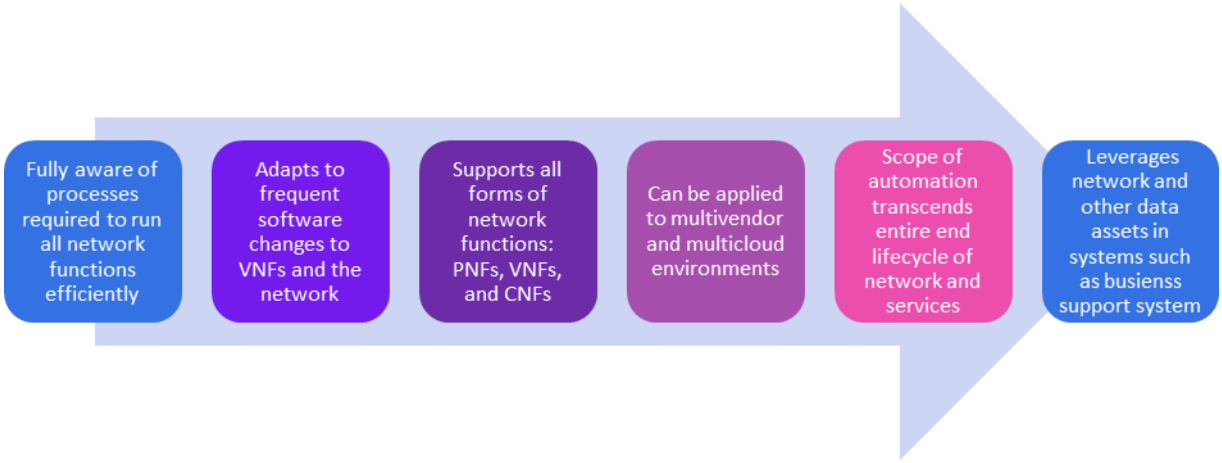
While we expect an acceleration in cloud-native network deployments in the next two years, CSPs must augment the level of automation to achieve the self-optimizing and self-healing properties that cloud-based, programmable networks promise. However, the addition of more automation comes with its own challenges if CSPs do not transform their operational practices.

Leveraging network automation to address network challenges

While CSPs have been implementing network automation for decades, the traditional static and domain-focused approach to automation is not suited to operating hybrid environments. Virtualized and cloudified networks are highly dynamic, requiring constant testing and monitoring to ensure network functions run effectively.

Networks must react quickly to customer demands. This means that to support the telco cloud, network automation will need to be intelligent, with visibility into the processes across network domains, network functions, and the underlying infrastructure (physical and virtualized). Key features that network automation will need to possess are summarized in **Figure 2**.

Figure 2: Key features of a network automation solution



Source: Omdia

At the core of every network automation solution is the ability to automate processes involved in the lifecycle of components within the telco cloud environment, including NFVI provisioning, VNF onboarding, orchestration (service creation, delivery, and management), and network operations. While CSPs are currently focused on automating the service and network lifecycle, automating the provisioning of cloud infrastructure is also important. Therefore, automation needs to occur at the NFVI (or cloud infrastructure) layer, the service orchestration layer, and the network operations layer.

Automation at the NFVI layer

For most NFVI implementations, the lifecycle management processes—including planning, procurement, delivery, provisioning, and VNF onboarding—remain complex, largely manual processes that take time and can be prone to errors. With growing demand for edge computing to support 5G in delivering a greater range of hosted applications and low latency use cases, it is imperative that CSPs automate their NFVI operations.

While the VNF testing and validation processes are getting more efficient, it can still take several weeks or months to onboard VNFs. Some VNFs require specific types of NFVI and virtualized infrastructure managers (VIMs) to function correctly. A lack of VNF interoperability between vendors remains an issue and is behind CSPs' continuing push for more open APIs. To address these challenges, VNF onboarding needs to be automated, with each vendor providing standardized blueprints for VNF onboarding including all forms of processes required to deploy and manage the VNF.

Setting up an NFVI that operates in a multicloud environment remains challenging for CSPs, especially establishing the connectivity between clouds. By automating NFVI provisioning and

leveraging concepts such as Infrastructure as Code (IaC),[1] CSPs can achieve faster time to revenue and increased efficiency for new capabilities coming with 5G, including network slicing.

Automation at the service orchestration layer

Service orchestration involves coordinating automated workflows required in the network service lifecycle from designing, creating, and delivering services. Increasingly, the service orchestrator also performs service assurance functions. This is to achieve closed-loop operations, with the orchestrator being aware of service level agreements (SLAs) associated with each service. To continuously guarantee service performance, the service orchestrator needs to track network issues that can affect services and trigger remedial workflows, for example by dynamically adjusting the infrastructure configuration.

Achieving these objectives for orchestration requires an end-to-end network approach that manages a broad range of services provided by multivendor network functions across multiple network domains and running in multicloud environments. Therefore, CSPs need orchestrators that leverage automation and cross-domain intelligence to understand how best to deliver and monitor the health of services in a way that fulfills customers' needs and assures high service performance.

Automation at the network operations layer

The evolving virtual network environment and demand for good customer experience place considerable pressure on network operations to become more proactive, such as performance monitoring, alarm management, troubleshooting, and network optimization. Changes to VNFs or CNFs will need to be tracked by network engineers in real time to limit the impact of these changes on services. Alarm monitoring should be automated and streamlined so network operations center (NOC) teams can focus on the most critical events.

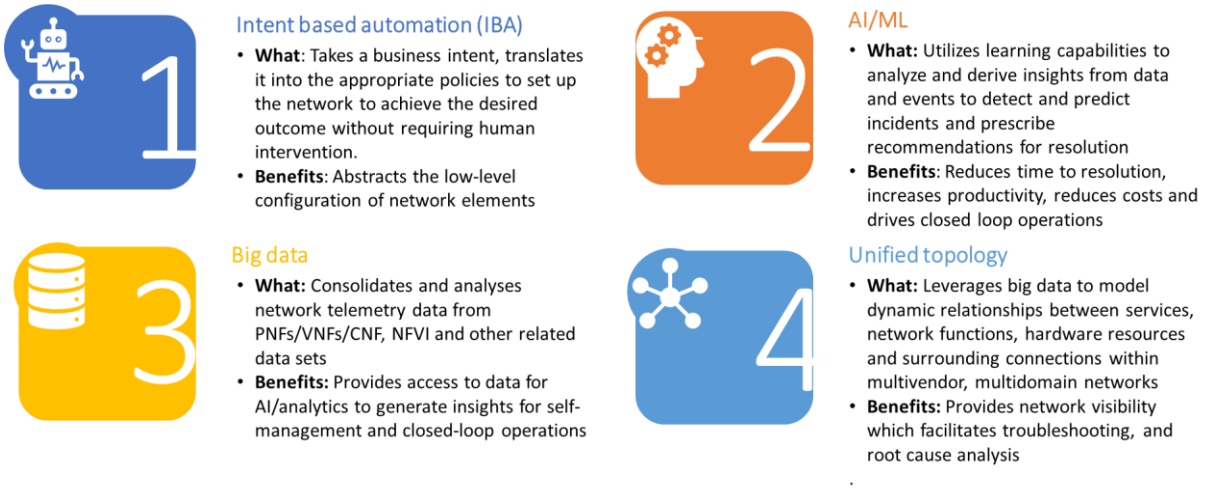
Automating these functions will require a consolidated view of the network resources and the services they support. This will enable cross-correlation of currently disparate network domains to speedily identify network incidents, their root causes, and ways to automatically remediate them where possible.

Enabling technologies for network automation

Effective network automation solutions will be driven by several technologies. **Figure 3** highlights four of these.

[1] Infrastructure as Code takes a model-driven approach that leverages code to provision and deploy resources in a data center to achieve a specific configuration or state.

Figure 3: Technologies to support end-to-end network automation



Source: Omdia

Some of these technologies are fast gaining the attention of CSPs as they realize the value they bring to executing their network automation strategies. AI and machine learning (ML), for example, are being explored by CSPs in automating service and network management. According to Omdia's ICT Enterprise Insights survey, nearly 80% of CSPs see the use of AI and analytics to automate network activities as an "important" or "very important" IT project for 2021, with nearly 60% of CSPs planning to increase investment in AI tools. Top AI use cases are expected to include network fault prediction and prevention, automation of end-to-end lifecycle management, and the management of network slicing.

Each of these technologies plays a unique role. However, the most value is derived when they are combined to achieve specific automation use cases. For example, IBA will derive most value from being combined with AI and analytics to inform the IBA engine when an intent fails or predict the likelihood of failure. By combining the capabilities of the IBA engine in a service orchestrator to fulfill a service request with the capabilities of AI to achieve service assurance, closed-loop operations can be achieved.

Automating NFVI provisioning

IBA can take on the laborious tasks of manually provisioning servers in a data center. By providing a data center model for a site to an IBA engine, and then utilizing declarative language to define the desired state of the cloud infrastructure, the IBA engine can determine how to achieve the desired site design. This model will include information regarding all processes and connections required to get the site ready to host VNFs and support various services.

In the event of network changes such as a network expansion (e.g., increasing compute capacity to support more customers or new services), the IBA engine can, based on the current view of the

network, identify what changes need to be made to achieve a new network state with the additional capacity.

End-to-end service orchestration

CSPs' ambitions for end-to-end service orchestration can be achieved by leveraging a combination of IBA, AI, big data, and topology. An IBA engine can accept service requests from service provisioning systems or service orders from a customer self-service portal. Based on the service intent, these are then defined using a standardized service model like the Topology and Orchestration Specification for Cloud Applications (TOSCA) model, and the IBA engine can orchestrate how the service should be deployed and monitored across the network. Network elements are configured by the domain controllers, and further checks can be performed by correlating the state of the network elements with their topology to ensure that the intent or service has been implemented effectively.

Verifying network behavior following network changes

As mentioned earlier, VNFs and CNFs will change regularly, so CSPs need to automate the testing and verification of services as well as the network workloads. IBA can enable CSPs to automate the analysis of network paths end to end to determine if a change has occurred and assess its impact on services. This can be done based on telemetry stored in big data platforms or collected directly from the network elements. AI algorithms can be applied to the datasets to confirm that network states and behaviors align with desired intent across all domains in the network. An example of such network behavior verification would be validating that the specified number of redundant paths from one network element to the next (e.g., one router to the next through an MPLS route) are available.

A key benefit of using IBA to support verification processes is that it abstracts the network complexity from the user and proactively identifies errors in the network that could lead to outages. It also avoids manual searches during root cause analysis and provides opportunity for the CSP to leverage its testing tools to automate network testing processes using DevOps.

Automated service assurance

AI and ML are being implemented by CSPs to facilitate service assurance functions. With alarm monitoring, for example, ML clustering capabilities can be applied to network event and alarm data to categorize and discover events. Events linked to service failures can be correlated with performance metrics to identify any failing devices and services affected, and where customer data is available detect those that will be affected. The result is a reduction and prioritization of alarms that NOC teams need to address, leading to increased productivity and better customer experience. By layering the clustered events with a dynamic network topology, the CSP gains visual representation of other devices affected by a network failure and likely root causes. Where known root causes are detected and a remedial process is identified, an automated workflow may be triggered, reducing mean time to repair (MTTR).

Baselining and detecting anomalies in network performance data can also be achieved using ML, and this can be done at a scale beyond human capabilities. AI and ML can enable thousands of KPI cross-correlations in real time, to discover "nontrivial" KPI relationships and abnormal behavior. Consequently, CSPs do not need to rely on rules to define thresholds, but can allow the ML model to track and report when network performance is not optimal.

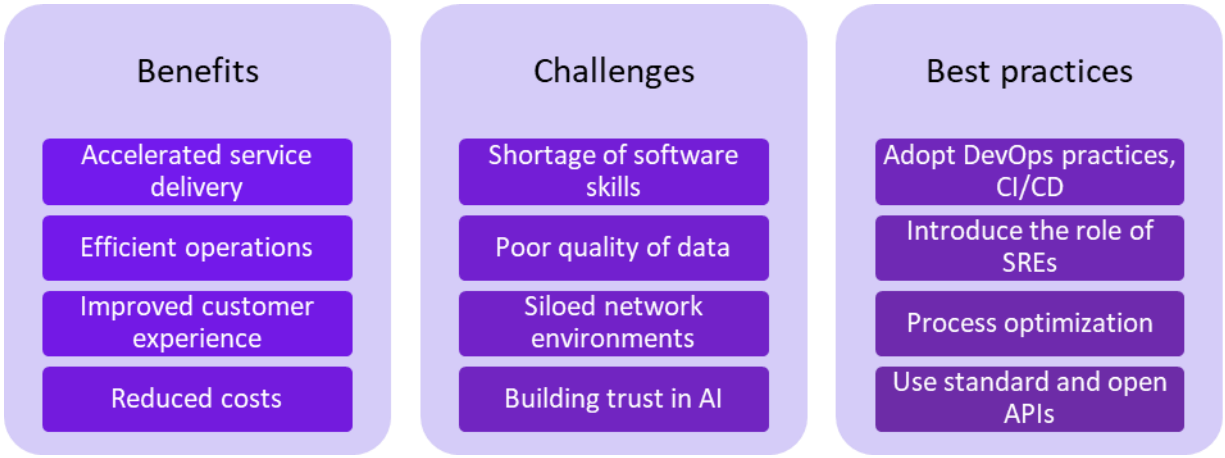
Optimization

Optimization of network and process parameters can be achieved using ML. ML models (e.g., neural networks) trained to optimize network performance based on several KPIs and current network parameters can track current network configurations to detect inefficiencies in existing network configurations. Based on the model's learnings, recommended changes to parameters can be raised and where possible automated workflows can be activated to adjust network parameters accordingly. This approach can also be applied to detect inefficient processes involved in creating and delivering services, and to recommend changes to optimize the processes and improve operational efficiency.

Benefits, challenges, and best practices

Figure 4 summarizes the benefits of network automation, potential implementation challenges, and best practices to address these challenges.

Figure 4: Benefits, challenges, and best practices for network automation



Source: Omdia

The reduced complexity in creating, delivering, and managing services and networks by leveraging end-to-end network automation creates opportunities for the accelerated rollout of new services. It also provides capabilities to improve customer experience and operational efficiencies.

However, current operating models and organizational cultures will limit the extent to which these benefits can be achieved. Operational transformation is therefore required to foster effective network automation. Network and service management teams should adopt DevOps practices, including integrating with CI/CD pipelines with related capabilities in the automated integration, testing, and deployment of VNFs and CNFs.

Before implementing automation, processes supporting every network function and service should be understood and optimized to achieve the required outcome. Feedback loops should be included when defining these processes (e.g., testing), so that when an automated process fails, a remedial

action to roll back to the previous operating state is activated or a fault is reported to the orchestrator. This is where the culture of SRE is important, as it involves continuously assessing processes for likely failures and taking action to avert them.

Finally, CSPs need to create a more open network environment, leveraging standard and open APIs to enable interoperability between network domains and systems and access to data to support AI. By implementing these best practices, CSPs can achieve a network automation strategy that is future-proof and constantly evolves to meet business objectives.

Conclusion

Implementing an end-to-end network automation strategy is critical to managing next-generation networks. While it may be challenging to deliver on this strategy, getting access to the right tool set, skill set, and information to transform organizational culture should become a priority. CSPs should move away from the status quo and be driven by the desire to reduce network complexity. This means leveraging AI and other technology assets to inject intelligence into current automation strategies, removing existing silos, providing direct access to data, and having well-defined processes.

CSPs will need to work with partners that are ready to innovate with them to source or acquire automation assets through IBA engines, big data platforms, and AI solutions. These vendors should position themselves as business partners to support the technical and organizational transformation needed to foster an end-to-end network automation strategy.

Appendix

Methodology

The information included in this report is based on primary research gathered through interviews, discussions, and inquiries with CSPs and IT vendors. Information in the report also includes survey insights from Omdia's 2020 Carrier SDN Adoption survey, and 2020 ICT Enterprise Insights survey. Secondary research from publicly available content and announced contracts, partnerships, and previously published research including Omdia's reports on AI and Network Automation and Network Functions Virtualization (NFV) Technology Forecasts, were also used in the development of this report.

Author

Adaora Okeleke
Principal Analyst, Service Operations and IT
adaora.okeleke@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.