Achieving a true Zero-Touch Network Vision

Automating the entire
service and network
management lifecycle

OMDIA

Contents

Summary

In brief

Today's communications service providers (CSPs) are plagued by increasing operational costs and demand for improved customer experience (CX). Zero-touch networks and operations have been identified as critical to addressing these needs through virtualization, artificial intelligence (AI), and automation. There are, however, business and operational implications that must be understood by all – including CSPs and their suppliers – as they chart a future of zero-touch networks.

Omdia conducted research in partnership with Ericsson to identify exactly what CSPs are trying to address using zero-touch networks. We interviewed key stakeholders within midsize to large CSPs (from regions such as the Americas, Europe, and the Middle East) and standards development organizations (SDOs) such as the European Telecommunications Standards Institute (ETSI), Metro Ethernet Forum (MEF), and TM Forum during the course of the research. These interviews were conducted to identify the direction in which the industry is moving to realize the zero-touch network vision. This report provides insights into those discussions including what business pain points CSPs face, how zero-touch networks will address these pain points, the enabling technologies required to address them, and the challenges associated with implementing them. It also explores the roadmap that CSPs should follow in order to evolve their networks toward a zero-touch world.

Omdia view

CSP networks are becoming increasingly complex and are reaching the point where they can no longer be reliably run by humans. CSPs also need to reduce costs and improve the flexibility and agility of networks to pursue new opportunities and respond to changing market conditions. Consequently, CSPs envision a zero-touch network that addresses these challenges.

> The zero-touch network is a simplified and software-based network platform, utilizing automation and AI to minimize human intervention in its operations. With the zero-touch network CSPs expect to deliver improved experiences to customers, because services meeting high quality standards can be created and delivered quickly. CSPs, on the other hand, look forward to increased revenue growth, because the zero-touch network enables them to deliver any service. In addition, the time and cost to create, market, deliver, and support new and existing services will be reduced. Operational efficiencies will also be achieved because of the robustness of the zero-touch network.

To achieve the zero-touch network vision, CSPs must invest in several technologies and capabilities to transform the network infrastructure, operations, supporting systems, and people skills. These technologies include software-defined networking and network

functions virtualization (SDN/NFV), end-to-end service orchestration, closed-loop automation, AI technologies, big data, and open APIs. In addition to realizing the benefits of the zero-touch network, other implications of adopting these technologies include the cost and time required to implement them. There are also changes that need to be made within the business to maximize the benefits of the zero-touch network. Emphasis should also be placed on CSP data assets, because they are critical to the functions of the AI algorithms that determine actions taken in the zero-touch network.

CSPs will encounter challenges as they embark on their zero-touch network journeys. The difficulties of change management, poor access to data, lack of interoperability, and the limited support from the vendor community are examples of these challenges. CSPs must take a wholistic and pragmatic approach to addressing these challenges. They must establish an effective roadmap that applies best practices when implementing technologies and capabilities required for the zero-touch network. This roadmap should provide a balance between the transformations that should occur in the network infrastructure, operations, systems, and employees' skill set.

Implementing the steps in this roadmap will not be easy. However, having key industry players – CSPs, the vendor community, and the SDOs – collaborate to accelerate the evolution of networks to being zero touch will be crucial. The journey to realizing zero-touch networks will take years, but it can be achieved with the right leadership, commitment, investment, and consistency in driving the vision.

Key messages

- The increasing complexity of the network is CSPs' top challenge as they build the network to meet growing demands for more services. They are looking to zero-touch networks to address this challenge: to simplify the complexity and minimize the level of human intervention required to manage the network and services.

- Technologies and capabilities such as virtualization, automation, AI, assurance, and orchestration are required to achieve the vision of zero-touch networks, with implications regarding cost and time for the change management critical to implementing them.

- With more network software and the legacy approach to managing networks, CSPs will experience challenges related to change management, standardization of data, service models, APIs, and the lack of interoperability across the CSPs' supply chain.

- CSPs should build a robust roadmap that focuses on transforming network infrastructure as well as business and network operations. This approach will ensure they are well positioned to meet their zero-touch network ambitions.

Recommendations

Recommendations for CSPs

- **Prioritize investment in technologies and capabilities needed to achieve the zero-touch network.** A zero-touch network will bring down operational costs. However,

costs will be incurred to attain the technical and operational maturity needed to run automated and flexible networks. CSPs must be ready to make this investment in order to take full advantage of the zero-touch network.

- **Focus on implementing the required change management.** Break down operational and network domain silos; implement a DevOps model to operate the network; upskill employees to prepare them for the demands of the zero-touch network.

- **Step up your participation in SDOs, open source (OS) communities, and projects focused on the zero-touch network vision.** By engaging in these organizations, CSPs (especially the larger ones) not only accelerate development of zero-touch networks but also enable their engineers to develop the skills and knowledge needed to support this new environment.

- **Take a stepwise approach as you evolve your networks to being zero touch.** Focus on solving one specific problem at a time: reduce costs, introduce new services and network capabilities quickly, or improve customer experience. Also aim to utilize your zero-touch network to deliver value to your mainstream services. Then move on to identify new services and customer segments to target.

- **Extend your partner ecosystem.** In addition to strengthening vendor partnerships, CSPs should build relationships with the web-scalers: AWS, Google, Microsoft, and Alibaba. These companies have succeeded in running zero-touch networks and have the requisite business development and innovation capabilities that drive business growth and customer value.

Recommendations for vendors

- **Provide open infrastructure using open APIs.** Vendors should provide these components, because they are critical to networks evolving to being zero touch. They also reduce costs associated with integrating your infrastructure within the zero-touch network.

- **Collaborate with industry players to define and adopt standards.** Vendors should align their products with the standards defined by SDOs and OS communities (driven by CSPs). It is crucial that entities such as data models, service definitions, and APIs are standardized, because they form the basis for a smooth evolution to zero-touch networks.

- **Take advantage of CSPs' demands for standards to strengthen current relationships.** While providing more open systems may limit vendor revenue potential, it helps fulfill CSPs' vision for zero-network networks. There are other opportunities to differentiate vendor offerings, either in the design of the standards-based software or in how you implement the standards. Identify additional services to offer to CSPs such as software development, systems integration capabilities, and support in using OS tools. As Verizon's Beth Cohen puts it, "Vendors are missing out on several opportunities to deliver value-add services to CSPs and they need to grab these opportunities."

- **Invest in building a robust service orchestrator.** This should have the capability to orchestrate all possible services offered and to do so across domains and vendor equipment. Fulfilling this request will be difficult; however, your engagements with OS communities can support development efforts to achieve this demand.

Recommendations for SDOs

- **Ensure the OS tools and platforms being developed align with standards.** This is critical, because CSPs are highly reliant on standards, frameworks, and OS tools to accelerate fulfillment of their zero-touch network vision.

- **Use your organization to fast-track development of zero-touch networks.** It is important to specify frameworks and standards and to test and validate them on live networks. SDOs should utilize their organizations as platforms to validate the value of these frameworks and standards. There are efforts to achieve this objective, for example, ETSI's OSM project and TM Forum's catalyst projects. However, it is important that these projects are positioned as platforms to test and advance development of zero-touch networks and not just opportunities to promote the standards.

- **Set up clear agreements with other SDOs.** SDOs need to ensure that the standards they define are clear and align to a similar goal to avoid conflict and confusion for the industry players being served.

# CSP business pain points and how zero-touch networks can address them

Increasing network complexity is CSPs' top business challenge

CSPs' top two business challenges are reducing operational costs and complexity and managing and monetizing 5G networks. Today's networks are a mesh of several technologies deployed to meet market demands. Migration to 5G will add further complications to CSP networks, adversely affecting how CSPs monetize and manage their networks.

Changes in network technology have been handled by adding new boxes instead of overhauling systems. Unfortunately, this trend has led to difficulties in launching new services to grow revenues, increasing operational costs and impairing customer experience. Operations such as service creation and delivery are inefficient, because they are highly manual and require several touchpoints that operate in silos. The result is prolonged time to market for new services, increased operational costs, and inability to respond quickly to demands for improved customer experience.

Figure 1: CSPs' top business challenges

CSP business challenges
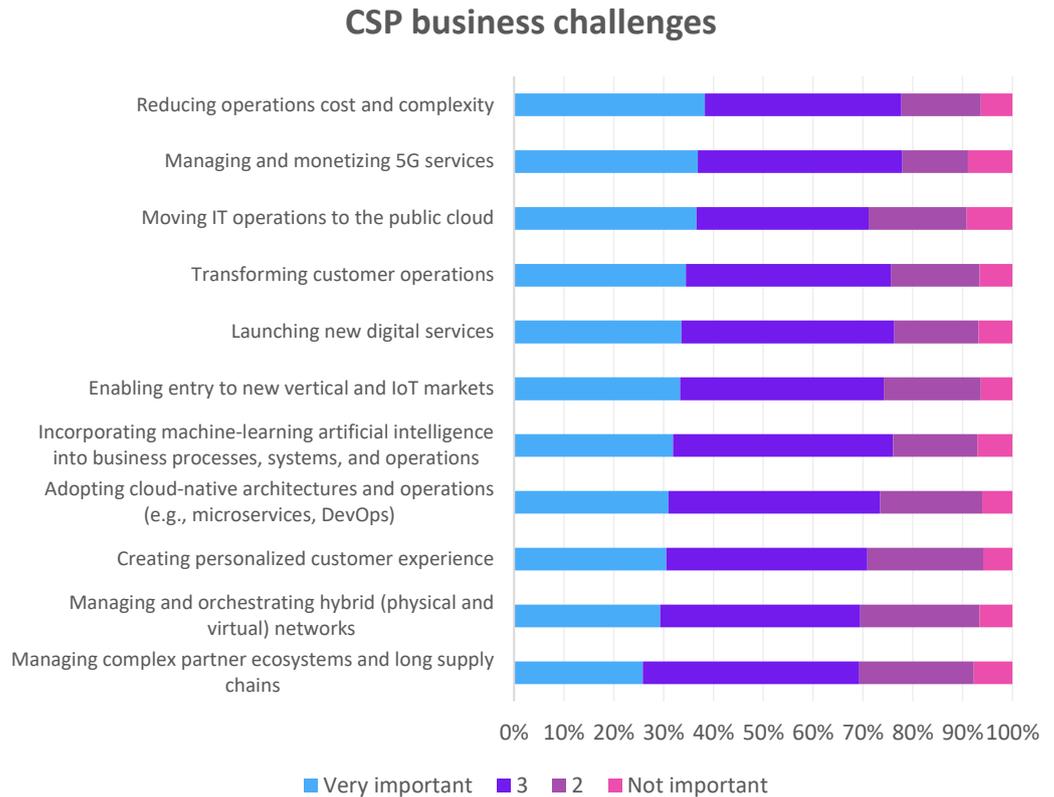
Source: Omdia *ICT Enterprise Insights 2019/20 survey*; n=420

The zero-touch network to simplify network complexity

To address these business challenges, CSPs need a versatile and flexible network that empowers them to innovate and transform the network and services quickly. CSPs are building the concept of the zero-touch network that abstracts the complexity of the network and simplifies network functions and operations, with the additional capability to deliver any service. The zero-touch network should ultimately deliver value to customers.

To achieve these objectives, the zero-touch network should possess the following key characteristics:

- The zero-touch network will have a highly automated underlying infrastructure, which requires minimal human intervention to operate it. Networks are not expected to be fully (100%) automated, hence the emphasis on minimal human intervention. According to the chair of the ETSI Industry Specification Group, Zero touch network and Service Management (ETSI ISG ZSM), Klaus Martiny, "Around 90% of automation of the network should be possible, but 100% will be difficult to achieve. We will see

over time what level of automation can be achieved from an investment and ROI point of view."

- It will utilize AI to provide intelligence needed to automate decision-making and the operations of the zero-touch network. This characteristic is important, because the scale of automation needed to operate the zero-touch network cannot be supported by a rules-based automation approach.

- The zero-touch network will be based on a horizontal platform that converges network technologies such as 3G, 4G, 5G, Wi-Fi, and so on and interconnects network domains (access, transport, and core) to work seamlessly in delivering any type of service.

- It will make use of a homogeneous network platform with programmable functions, not functions that are hardcoded into the network nodes. The result is a flexible network infrastructure that can be easily adapted to deliver any service to customers or respond quickly to market changes.

- It will easily be accessed by CSPs' customers, for example, enterprises to design the services they need and define the telco capabilities required to deliver the services. All the CSP needs to do is parse these requirements to the network and have them automatically fulfilled.

- Every network domain will support complete lifecycle management of the services it provides (including closed loop). They will also expose their services using standard APIs, thereby reducing operational tasks to simple changes in network parameters or reuse of existing services.

The scope of automation within the zero-touch network

Automated configuration, management, and operations of physical and virtual devices is a crucial function of the zero-touch network. The scope of this automation will span four key layers – network and resource automation, service automation, CX automation, and business and ecosystem automation – as shown in Figure 2:

Figure 2: CSP automation landscape
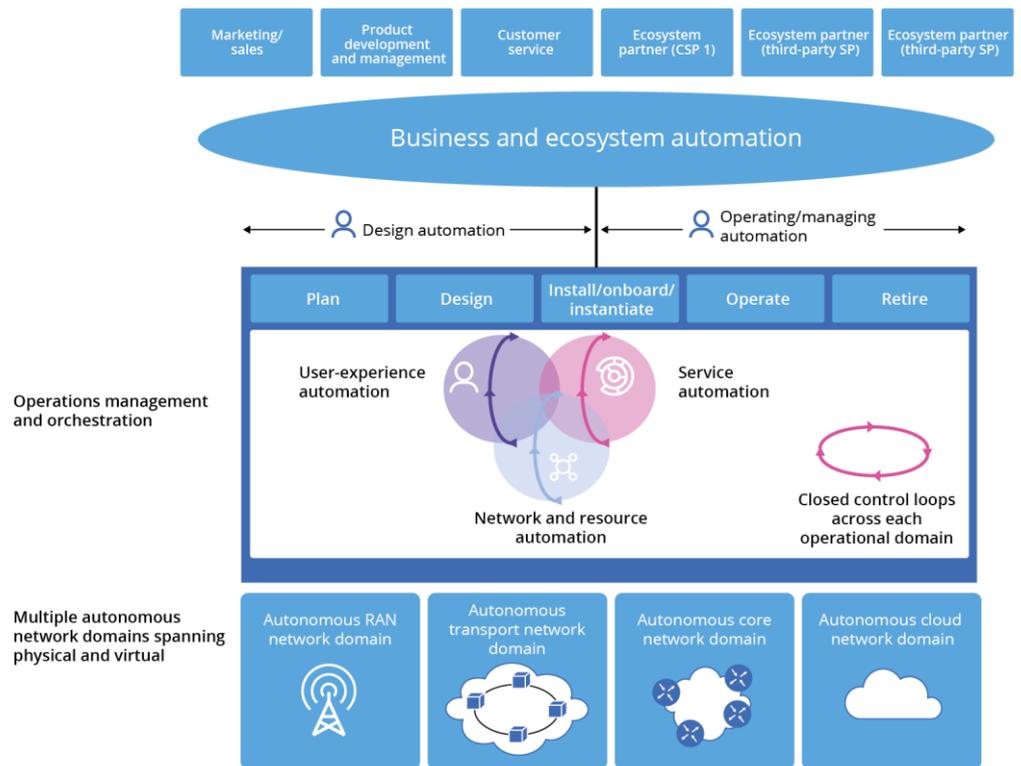
Source: Omdia

- **Network and resource automation.** This means automating the lifecycle management of network resources: configuring, instantiating, managing, and retiring the network resources.

- **Service automation.** This involves automating the end-to-end lifecycle management of services delivered by one CSP or multiple CSPs.

- **User experience automation.** This focuses on automating the entire customer journey to minimize the touchpoints that customers encounter when requesting or consuming any service. It also involves automatically tracking the entire customer experience to preempt customer actions and take proactive steps to deliver high-quality experience. This type of automation is yet to be defined by the industry.

- **Business and ecosystem automation.** This refers to automating business interactions and activities between different players involved in delivering services that CSPs provide. These include pricing, ordering services, and generating the business case for the service to be delivered. It also includes automatically triggering marketing campaigns based on service-consumption patterns.
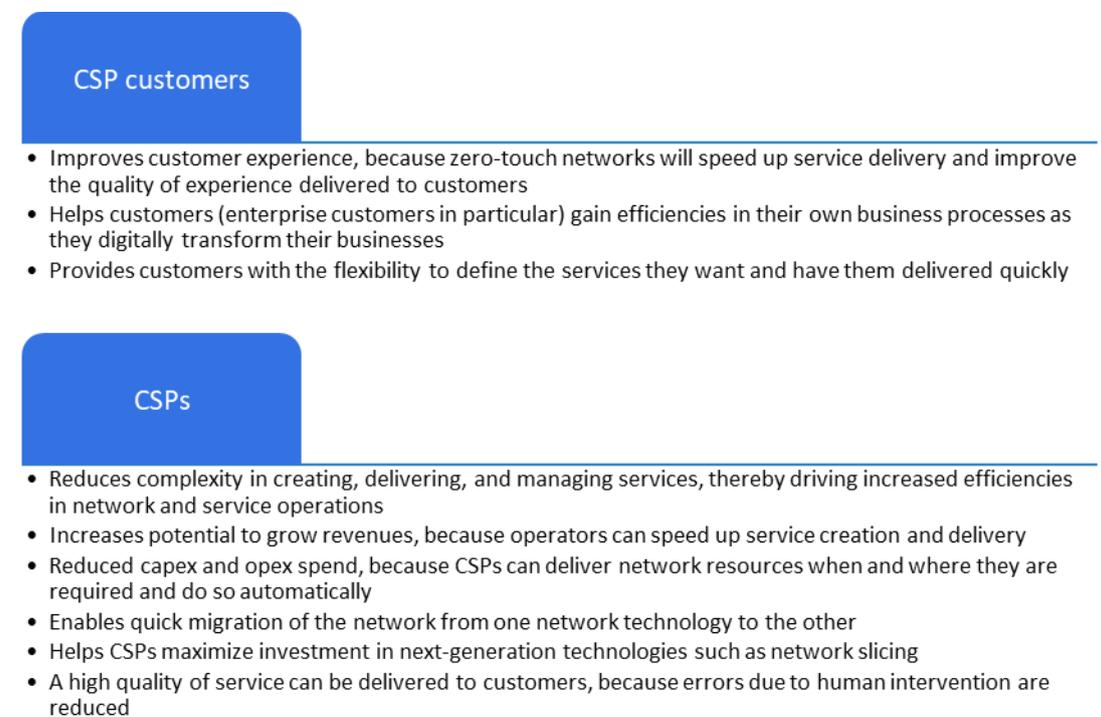
More advancement is seen in the network/resource automation layers: CSP spend is highest at this layer compared to other parts of the business. However,

network/resource automation is not all that is required to achieve CSPs' cost reduction and agile network transformation objectives; all four levels of automation are needed.

Benefits of the zero-touch network

Figure 3 summarizes the key benefits that the zero-touch network will deliver to both CSPs and their customers.

Figure 3: Benefits of zero-touch networks

CSP customers

- Improves customer experience, because zero-touch networks will speed up service delivery and improve the quality of experience delivered to customers
- Helps customers (enterprise customers in particular) gain efficiencies in their own business processes as they digitally transform their businesses
- Provides customers with the flexibility to define the services they want and have them delivered quickly

CSPs

- Reduces complexity in creating, delivering, and managing services, thereby driving increased efficiencies in network and service operations
- Increases potential to grow revenues, because operators can speed up service creation and delivery
- Reduced capex and opex spend, because CSPs can deliver network resources when and where they are required and do so automatically
- Enables quick migration of the network from one network technology to the other
- Helps CSPs maximize investment in next-generation technologies such as network slicing
- A high quality of service can be delivered to customers, because errors due to human intervention are reduced

Source: Omdia
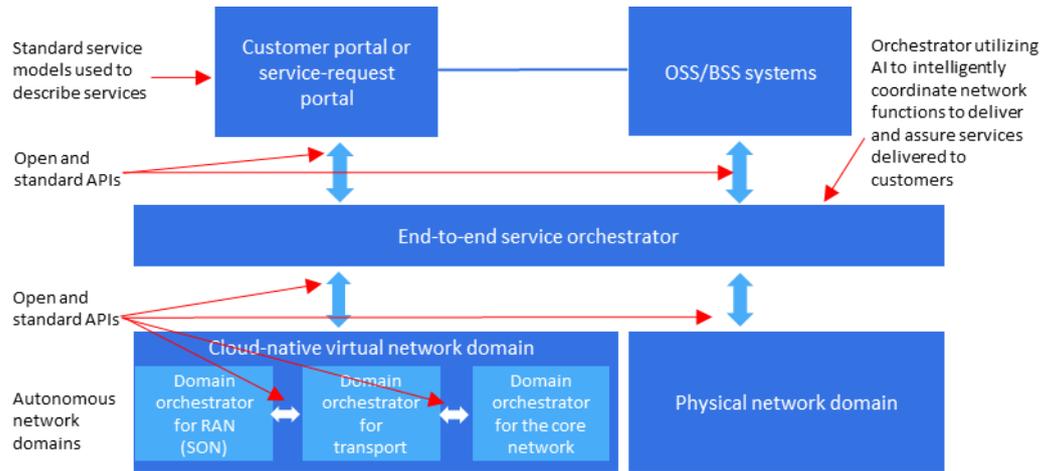
Technologies and capabilities required to achieve zero-touch networks

CSPs' networks will change massively as they pursue the zero-touch network vision. Networks will transform from being hardware to software driven, utilizing cloud computing principles. This approach will enable them to benefit from the speed, flexibility, and agility that web-scalers currently enjoy when creating and modifying services. The network and operations will become focused on services delivered by the network resources, not just the functions. These services will need to be composed and decomposed from network resources quickly. Most importantly, the management and orchestration of network and services in this zero-touch network will be driven by closed-loop automation.

To realize these changes, CSPs will need to invest in technologies and capabilities that transform the network infrastructure, the operations, and the skill set needed to manage and monetize the zero-touch network. These technologies include SDN/NFV, orchestration, AI and analytics, and software development skills. Table 2 provides commentary on these technologies and capabilities, and Figure 4 provides a summary of where these technologies and capabilities are applied within the structure of the zero-touch network.

Figure 4: What the zero-touch network would look like and the key technologies that enable it

Source: Omdia

Implementing these technologies and capabilities does not require a complete rip and replace of existing network infrastructure, because CSPs must protect the legacy services running over the existing network. However, a stepwise approach must be taken by CSPs when implementing these technologies to migrate existing services to the zero-touch network environment.

Implications of implementing these technologies

Investing in these technologies and capabilities to transform networks to being zero touch comes with benefits to CSPs' businesses and operations as well as challenges and responsibilities. These are summarized in Table 1.

Table 1: Business and operational implications of implementing technologies for the zero-touch network

Business implications	Operational implications
Increased pace of service creation and delivery reduces time to market for new services.	Roles associated with practices to be automated will become redundant.
Improved customer experience as CSPs become agile and proactive in responding to customer needs.	New roles and functions with new skills will be required to support the zero-touch network.
Costs will, however, be incurred in the short to medium term to implement these technologies and capabilities.	Operational practices need to change to align with the agility needed to operate the zero-touch network.
Strong leadership will be needed to represent the interests of the zero-touch network to make sure that the project is funded, is moving in the right direction, and is yielding the desired outcomes.	OSS/BSS systems should align with the capabilities and operations of the zero-touch network.
Service delivery methods will need to change to enable customers to benefit from investments made in transitioning to a zero-touch network.	Data will become a critical component of all functions supporting the zero-touch network. Data supports the extraction of insights needed to derive intelligence to automate the functions of the zero-touch network.

Source: Omdia

Key challenges in evolving to zero-touch networks and how to address them

Difficulties with change management

To successfully achieve the zero-touch network vision, CSPs need to make changes such as

- taking a more consolidated approach to managing the network

- following a software-driven approach to developing and managing the network

- creating an operational structure that relies on automation to perform mundane and repetitive tasks

- having a workforce that is versed in software development skills

- redefining the business model to maximize investment in building the zero-touch network.

The majority of the respondents who participated in our research see change management as being a top challenge given CSPs' legacy and siloed approach to managing networks and the business. CSPs will need to go through a company-wide culture change to align with the demands of the new network if they are to enjoy the benefits of zero-touch networks.

Take a collaborative and proactive approach to managing the network
Adopt a DevOps and service-based approach to managing networks
CSPs should take a more agile and collaborative approach to implement the changes needed to support the zero-touch network. Moving to a DevOps model will help remove existing silos and provide a more unified environment in which development and operations teams can collaborate to build, test, and release network software more quickly and reliably. Klaus Martiny of ETSI ISG ZSM indicates that "without the combination or close working between the engineers and the operations teams, delivering optimized network lifecycle management will be difficult." Also, organizations managing the different network domains need to work together closely. Existing silos between these organizations should be removed. Each network domain needs to define all the services it provides using a standard service model to define the granularity of the parameters of the service. These services can then be exposed and requested via

standard APIs. This approach will facilitate network automation and simplify service operations.

Business and operating models should be more proactive and customer centric
CSPs should be more proactive in creating new services, business models, and operations with a view to delivering personalized experiences to customers. The zero-touch network should enable customers to create services they want and have them delivered to the highest quality. A way to fast-track this change to being more customer centric is for CSPs to build relationships with the web-scalers AWS, Google, Microsoft, and Alibaba. These companies have succeeded in running zero-touch networks and have the requisite business development and innovation capabilities to enhance operations and drive business growth and customer value from these networks.

Lack of interoperability

The lack of interoperability within CSPs' broad ecosystem of partners limits the extent to which CSPs can achieve the zero-touch network vision. Some of the challenges that arise as a result of this issue include

- **potential slowdown in the pace of development of zero-touch networks:** CSPs find it difficult engaging with other vendors or startup organizations to bring in innovative approaches that support their zero-touch network vision, and as a result, progress in achieving zero-touch networks could be hindered

- **increased cost associated with introducing innovation:** CSPs incur costs from systems integrators each time they need to introduce a new feature or capability within their networks, which impacts on the availability of budgets to drive further innovation

- **limited access to data** required to train AI models to enable intelligent automation.

Adopt systems with standard and open APIs
Having standardized and open systems and APIs that enable network devices to interoperate is important. This explains why OS projects (such as ONAP and ETSI's OSM) that involve the use of OS tools are gaining a lot of traction within the CSP community. While there are limitations to the extent of the "openness" of some of these OS platforms, the pace of development is much faster if the tools are open and utilize standardized APIs. CSPs and vendors need to adopt these systems with standard and open APIs to facilitate innovation and realization of zero-touch networks.

Nonalignment and slow development of standards

Observations made by some of the research participants indicate that the pace of development and testing of standards is slow. The development of OS network automation tools including ONAP and ETSI's OSM, on the other hand, is not aligned. The effect of these observations is confusion for CSPs and vendors creating products based on these standards.

Agree on a standard automation framework

One way for vendors and CSPs to address this challenge is to develop products that align with standards being backed by either most CSPs or the majority of top-tier CSPs. Another option is to perform an exhaustive and unbiased analysis of these platforms to determine which fulfills the core requirements for the full end-to-end network and services. Regardless of which option CSPs decide to take, they need to agree on the automation architecture or infrastructure to implement. This will make implementation from a CSP's or vendor's perspective easier.

Data quality challenge

Data is key to deriving the intelligence needed to achieve closed-loop automation in zero-touch networks. Sadly, the multivendor environment that CSPs run and the nonstandardized data assets generated by the network make it difficult to get the data in a format that aligns with the requirements of the AI models.

Standard interfaces and data management practices are critical

In addition to defining standard interfaces for ready access to data, defining a standard approach to storing and managing these data assets is crucial. This standard approach ensures that high-quality data is available to operate the zero-touch network. Telefónica, for example, places a high premium on its data infrastructure and is progressing with its zero-touch network. The CSP is building strong governance capabilities to ensure data is accessible and useful in deriving the required insights.

Challenges associated with CSPs' legacy OSS/BSS systems

Existing OSS/BSS systems cannot support zero-touch network operations. They are massive monolithic systems that are inflexible and take time to modify when a new service is to be launched.

Redesign OSS/BSS as microservices-based systems

To effectively manage the zero-touch network, these systems should be re-architected as microservices-based applications. With this architecture, changes to these supporting systems can be made quickly by modifying the required microservices within these systems each time a new service is to be launched. This transformation reduces time to market and costs for new service launches.

Delay from vendors in delivering solutions that support zero-touch networks

Most CSPs that participated in the research see their vendor partners as being slow to support their zero-touch network vision. This is seen in the vendors' reluctance to implement standard capabilities such as open APIs, data, and service models. These CSPs also perceive their vendors as being slow to develop end-to-end orchestration solutions that coordinate all services across all domains. Meeting these demands is daunting for most vendors given the lack of open systems to communicate with the service orchestrators they provide.

Vendors should see themselves as partners, not just providers of technology
Collaboration and partnership between CSPs and vendors is critical to ensure the right solutions and capabilities for zero-touch networks are provided. The vendor community needs to commit to providing standard and open network equipment and systems. With this commitment, CSPs' demand for end-to-end service orchestration capabilities might be met.

Building trust in the platform to run the network

CSPs need be able to trust machines to handle operations that were previously executed by humans. They need visibility into the functions of automated systems to identify, troubleshoot, and resolve problems. They also need to understand how decisions are made by the AI systems. Unfortunately, there is limited visibility into the functions of automated systems, especially AI-based systems, which impacts the level of trust that CSPs will have in them. The effect of this lack of trust is reduced speed in implementing the technologies and capabilities needed to achieve the zero-touch network.

Exhaustive software testing and transparency of AI models must be prioritized
The trust challenge can be addressed by spending more time coding the functions that the network performs and testing them until the platform is able to handle the task at maximum levels.

A high level of transparency of the inner workings of AI models used to automate the network will also be beneficial in building trust. The operations of algorithms must allow some level of supervision from humans to interject the functions of these algorithms to ensure that policies are always observed. According to Vodafone's Neeraj Pandey (VP, Network Engineering and Delivery), "People may be slow, but they are much wiser than machines."

Fear of job losses

CSP employees remain skeptical about the effect that a zero-touch network would have on their current roles. Consequently, they are still hesitant to adopt any approach that allows the CSP to move forward in realizing its zero-touch network vision.

Raise awareness of the value of zero-touch networks to employee productivity
Educate employees on the benefits of zero-touch networks to their productivity. For example, automation will enrich their productivity levels and create opportunities to enhance skills. A study by the World Economic Forum in 2018 highlighted that the introduction of automation to businesses using AI will create about 60 million new jobs. While this number is not limited to telecoms, it does indicate the opportunities for employees to upskill and take on new roles, for example, training, configuring, retuning, and managing AI models; establishing governance and compliance; and setting up the ethical standards for the AI models driving automated workflows. CSPs will allay employees' fears of machines taking over their roles by identifying ways to reskill the existing workforce to take on these new roles.

Roadmap to achieving the zero-touch network vision

The roadmap should align with business priorities and maturity of network virtualization
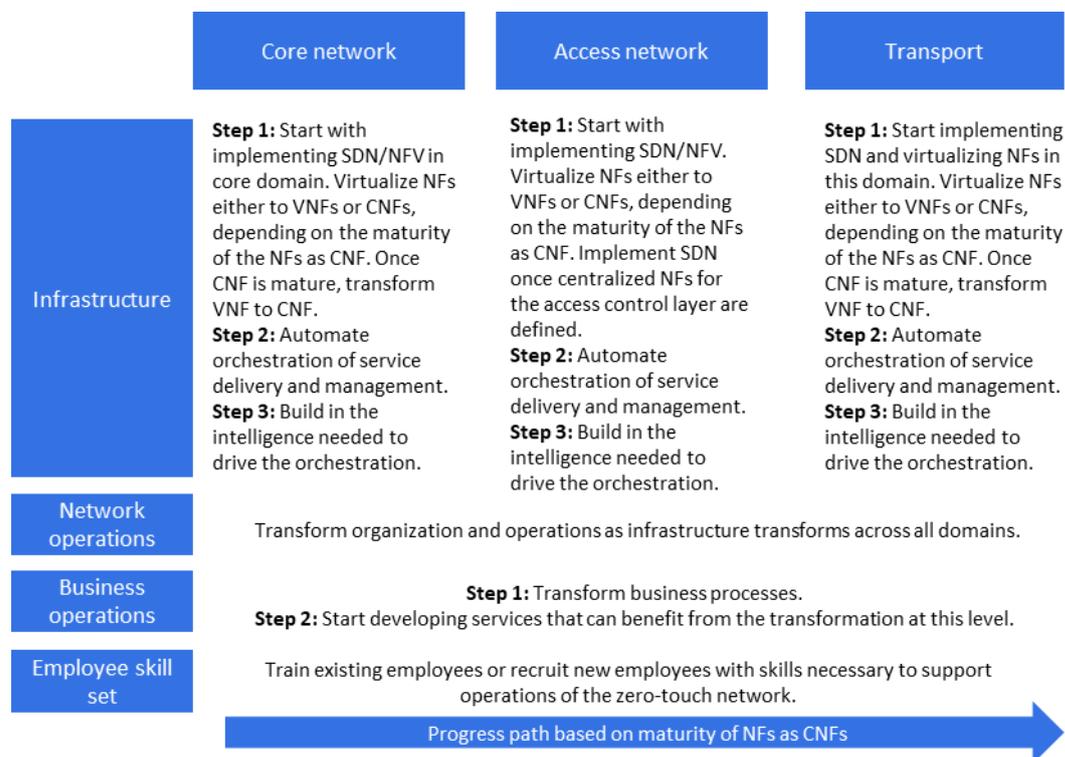
The roadmap to achieving the zero-touch network should follow the following principles:

- Ensure business objectives remain the core target of this transformation exercise.

- Align with the maturity of network virtualization across domains.

- Ensure that standards are observed.

The journey to the zero-touch network should start with the network infrastructure. According to CenturyLink's CTO Andrew Dugan, "Automation of the network must be the first step in the roadmap towards zero-touch network and then the automation of services." However, to facilitate network automation, the network needs to be transformed to a cloud-native platform. The gains of each step of the network transformation should be transferred to service creation and delivery processes as quickly as possible. Introduce new services or enhance existing services with the new network capabilities. As the network is being transformed, operations, processes, and employee skill set should change with it.

Taking this approach can potentially drive a quick ROI with less capital at the beginning of the journey as customers start enjoying and paying for the services generated from the network. With the required operations and skill set to support new network capabilities, the CSP is well positioned to support new services. The CSP can also utilize revenues from new services to further develop and fulfill the zero-touch network vision. Figure 5 provides a summary of the roadmap that can be adopted in realizing the zero-touch network.

Figure 5: Roadmap to achieving the zero-touch network

	Core network	Access network	Transport
Infrastructure	**Step 1:** Start with implementing SDN/NFV in core domain. Virtualize NFs either to VNFs or CNFs, depending on the maturity of the NFs as CNF. Once CNF is mature, transform VNF to CNF. **Step 2:** Automate orchestration of service delivery and management. **Step 3:** Build in the intelligence needed to drive the orchestration.	**Step 1:** Start with implementing SDN/NFV. Virtualize NFs either to VNFs or CNFs, depending on the maturity of the NFs as CNF. Implement SDN once centralized NFs for the access control layer are defined. **Step 2:** Automate orchestration of service delivery and management. **Step 3:** Build in the intelligence needed to drive the orchestration.	**Step 1:** Start implementing SDN and virtualizing NFs in this domain. Virtualize NFs either to VNFs or CNFs, depending on the maturity of the NFs as CNF. Once CNF is mature, transform VNF to CNF. **Step 2:** Automate orchestration of service delivery and management. **Step 3:** Build in the intelligence needed to drive the orchestration.
Network operations	Transform organization and operations as infrastructure transforms across all domains.		
Business operations	**Step 1:** Transform business processes. **Step 2:** Start developing services that can benefit from the transformation at this level.		
Employee skill set	Train existing employees or recruit new employees with skills necessary to support operations of the zero-touch network.		
	Progress path based on maturity of NFs as CNFs →		

Source: Omdia

Infrastructure

- **Virtualize the network and aim for a fully cloud-native network infrastructure.** Consider what network functions (NFs) across domains gain the most benefit from being virtualized, and start your virtualization journey with these NFs. Transform NFs either directly to cloud-native functions (CNFs) or to virtual network functions (VNFs) and then to CNFs, depending on the maturity of NFs as CNFs. Virtualize centralized NFs first and then move to distributed NFs. This principle applies to all network domains. The transport layer will leverage SDN mainly for its transformation.

  - **Benefits.** Cloud-native networks fast-track network evolution to zero-touch network, because automating CNFs is easier and quicker to achieve. They also hasten attainment of benefits such as accelerated time to market, reduced total cost of ownership and future-proofing of innovation cycles. With cloud-native architecture, CSPs can rapidly deploy new services to customers. It also enables the smooth adoption of the DevOps operating model. With a cloud-native network, CSPs can expand their partner ecosystems to include more agile, innovative companies.

- **Automate the end-to-end orchestration capabilities.** Take a standards-based approach to automating service and network orchestration. Alongside that, plan to transition from static network inventory to a dynamic and federated inventory to

facilitate functions of the orchestrator. Standardizing service models and APIs should be included in this phase.

- **Benefits.** By automating the orchestration functions, service providers can solve challenges associated with managing physical and virtual domains, reduce operational costs, and drive faster creation and delivery of new services. Quality of experience will improve as errors due to human intervention are reduced.

- **Build in the relevant intelligence to inform the functions of the end-to-end orchestrator.** Invest in AI technologies to provide this intelligence to achieve closed-loop automation of the fulfillment and assurance functions of the orchestrator. Build a strong data infrastructure that ensures quick access to data sets for analysis.

  - **Benefits.** This step transforms operations from being reactive to being proactive. AI-driven intelligence solutions can also scale well to support broader automation use cases.

Network operations

- **Perform change management in network operations alongside the network transformation.** Transform operations as you transform the network. Restructure workflows to efficiently run the software-based networks. DevOps needs to become the de facto operating model to facilitate innovation of NFs. AI capabilities need to be brought in line with the operations to transform the way that the network is operated and solve key pain points.

  - **Benefits.** Making changes to the network and managing the network "in code" is quicker, easier, and less costly than physically "ripping and replacing" or updating hardware and configuring physical switches.

Business operations

- **Transform existing services, business operations, and processes in line with the new infrastructure capabilities and the needs of the customers.** As a key milestone in the network transformation journey is achieved, transform services and business processes, particularly product management, marketing, and sales. This ensures that new network capabilities are used as soon as possible to enhance existing offerings while seeking out new services to offer. Product development teams need to take a more agile approach to rolling out new services. Marketing, on the other hand, needs to identify how best to target these services at customers to generate maximum ROI.

  - **Benefits.** This enables CSPs to drive value to the customers, thereby achieving ROI for the zero-touch network.

Employee skill set

- **Reskill the workforce.** Build a workforce with the requisite skills (e.g., software development skills, service and algorithm modeling) to adapt to and manage the zero-touch network.

- **Benefits.** Having the right skill set in place to manage the zero-touch network will reduce the time it will take CSPs to start running more efficient and flexible operations. The workforce is also ready to take on any issues regarding operations of the zero-touch network, reducing the costs associated with getting external resources to address them.

The roadmap should also recognize that the legacy infrastructure will be required to keep the lights on for the traditional services. However, there needs to be a plan to migrate these services from legacy infrastructure to the virtualized network environment over time.

Technology definitions

Table 2. Technologies and capabilities required to achieve the zero-touch network

Technologies and capabilities	Definitions and commentary
SDN/NFV	At the core of the zero-touch network are SDN and NFV. These technologies transform NFs from hardware to software; NFV decouples the NF from the hardware in the form of VNFs, while SDN disaggregates control functions from the forwarding functions. With NFs in software, automating configuration, provisioning, and management of the network becomes easier, thereby reducing the costs and time taken to perform these functions. NFV also enables different network applications to share the same hardware.
	The true benefits of NFV/SDN are realized when the NFs are cloud native. This means that they are developed using microservices, running within containers such as Docker and managed using container orchestration systems such as Kubernetes. As cloud-native network functions (CNFs), true dynamic scaling and elasticity can be achieved. Continuous integration, continuous delivery (CI/CD) principles can also be applied to accelerate innovation. The result is a flexible and agile network infrastructure with the capability to meet market demands and reduce the time to market for new services.
Orchestration	Orchestration is crucial to the functions of the zero-touch network, because it coordinates the lifecycle management of all services delivered over the physical and virtualized network environments. These services could be network services or customer services. Whatever the service type, the orchestration capability should operate automatically in a closed-loop fashion, achieving functions such as service coordination and instantiation, service monitoring, and service scaling.
	CSPs have varying views regarding the extent of control a service orchestrator can have. BT, for example, highlighted at the Zero Touch Automation Congress in 2019 that it does not believe in the notion of a "single orchestrator that knows everything about the network." Therefore, it is architecting its zero-touch network with one orchestrator for each domain and having hierarchical orchestrators overseeing the lifecycle of services provided end to end. Vodafone's Neeraj Pandey, on the other hand, indicates that "the orchestrator should be able to understand and control all services across all network domains."
Policy engine	The policy engine generates and distributes policies, conditions, requirements, constraints, attributes, or needs that must be provided, maintained, and/or enforced within the network. These policies enable actions to be taken based on triggers or requests. The policy engines also assess conditions, selected policies, and outcomes of all policies before deciding what policy should be taken. These policies or rules can be rapidly modified based on intelligence generated from the network.
AI and analytics	These technologies provide the intelligence that drives the automated orchestration and management of the network. AI algorithms, for example, can be applied to automate mundane tasks by deriving key learnings from the network data. By analyzing the telemetry and events data regarding how the network is programmed to act upon certain events, they determine the right actions to take that trigger a desired outcome in the network, for example, determining configuration changes to make to scale up or scale down network resources or remediate a network fault, thereby reducing the need for humans to perform mundane tasks and enabling the network to adapt to changes within the network.

Big data lake or data infrastructure	These are required to provide a standard framework to collect, store, manage, and secure data from the network. Analytics and AI algorithms can be deployed on the data within the big data lake and insights passed on to the orchestration to initiate an action. The data lake structure could be centralized or distributed with a view to ensuring that the data required to drive the intelligence and automation of the zero-touch network is easily accessed.
Unified network inventory and topology	These capabilities facilitate the functions of the service orchestrator by providing a multivendor, multidomain view of the network elements (physical and virtual). This capability enables the service orchestrator to view the entire network as a single network. Operational savings and reduction in the time it takes to onboard network components are achievable using unified network inventory and topology. Following the creation of a unified network inventory solution, Ravi Ramachandran, platform director of BT OSS, indicated that the accuracy of the telecoms network inventory is critical to achieving automation. He also added, "The accuracy can only be leveraged by having a single resource inventory system. With a single version of the truth, there is quicker time to market and better network planning and utilization, which leads to opex and capex savings." (TM Forum.)
Adopting a model-driven network architecture	The model-driven architecture specifies the configuration, relationships, dependencies, and sequencing of resources to be used in delivering a new service offering. Using these models (or templates) simplifies the new service creation process by making it easy to create reusable building blocks that may be used as resources for other new services. These models can be created using standard modeling languages or scripts such as Topology and Orchestration Specification for Cloud Applications (TOSCA) for service description or YANG models for defining and configuring network devices. Vodafone is one CSP that is moving to the model-driven architecture: it is using TOSCA and YANG templates to standardize service definitions and configuration of network nodes to deliver services.
Standardized APIs, service models, and data models	Standardization fosters interoperability between interworking multivendor network components and cloud environments. Without this capability, achieving the zero-touch network vision will be expensive and take more time. Standardizing key components such as APIs, service models, and data models is critical to enabling interoperability. APIs enable communications between domains and communications between orchestrator, domain controllers, OSS/BSS systems, and the customer-facing portals. Service models facilitate the creation and lifecycle management of services. Customers can utilize these models to define their service requirements and have the network automatically fulfill and assure the service based on these requirements. Standard data models, on the other hand, facilitate the implementation of AI models, because pretrained models can be implemented across network environments. The various industry standards organizations are forging ahead with defining standards: • The ETSI ISG ZSM has defined a new end-to-end framework that enables agile and efficient management and automation of emerging and future networks and services. • MEF standardizes the way connectivity services such as MPLS and Carrier Ethernet are defined and orchestrated. For example, the MEF Lifecycle Service Orchestration APIs (LSO APIs) define how services are orchestrated. MEF also certifies CSPs and vendor equipment delivering these services. • The TM Forum Autonomous Networks Project aims to develop a common understanding and consensus on the autonomous network concept. It also defines how automation is classified to achieve simplified telecoms network infrastructure, automated and intelligent operations, and innovative services.
Software development skills and practices	Network engineers must develop software skills to manage the network effectively. With NFV/SDN abstracting the control functions of the network from the hardware, more of their activities will concentrate on modeling within software the key functions the network is required to provide to support services. They need to adopt DevOps practices to speed up the evolution of NFs to fulfill business objectives and deliver value to customers.

Source: Omdia

Appendix

Author

Adaora Okeleke
Senior Analyst, Telecoms 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