analysys
mason

END-TO-END NETWORK ORCHESTRATION: CSPs ARE TAKING A STEPWISE APPROACH

Anil Rao, Hansang (Andy) He

JULY 2019

analysysmason.com

Contents

1 Executive summary

Network function virtualisation (NFV) and software-defined networking (SDN) technologies are transforming the way networks are designed, built and provisioned. At the heart of this transformation is the expectation that these technologies will enable communications service providers (CSPs) to achieve high levels of network automation to: reduce service delivery times from months to days or even hours or minutes; and automate the network optimisation and day-to-day operations to guarantee the contracted service levels and quality of service.

Based on the cloud principles of infrastructure flexibility and on-demand resource optimisation, NFV and SDN provide the key networking foundation for automation. However, to fully realise these benefits, CSPs require next-generation network management software, commonly known as network orchestration (NO). CSPs are taking two broad paths towards implementing NO – the NFV path for the service lifecycle management and orchestration of virtual network functions (VNFs), and the WAN SDN path for software-defined control and automation of the wide-area network (WAN). These two paths ultimately converge with the implementation of a fully integrated cross-domain network orchestration (CD-NO) system that performs the combined function of lifecycle management and WAN SDN across networking domains to create and provision services end-to-end.

This white paper presents the findings of primary research (a survey of, and interviews with, CSPs) conducted by Analysys Mason to assess the status of NO implementations worldwide, the preferences of CSPs when choosing network orchestrators and the challenges encountered during the implementation. The key findings of the survey were as follows.

- The survey unequivocally proved that CSPs worldwide are considering or deploying some form of NO to operationalise NFV- and SDN-based networks.

- More than half of the CSPs surveyed said that network automation was a top-3 strategic initiative, and it was the main motivation to deploy NO.

- Service lifecycle management, and network and service configuration automation were the most common use cases for deploying NO.

- Co-development with a preferred vendor partner was the most popular choice for building NO, with CSPs stating that they would like to retain key domain knowledge while leveraging the supplier's expertise.

Based on our ongoing research in the area of network automation and orchestration, it is evident that most CSPs are taking a stepwise approach to deploying CD-NO. As CSPs gradually introduce new NFV and SDN domains, the new and changed components must be integrated with the adjunct components, including the existing orchestration systems. Due to the diverse nature of CSPs' virtualisation environments, software components will require high levels of customisation to make virtualisation environments fit for purpose. To achieve the desired results in such a dynamic and complex networking environment, even as they support existing services, CSPs will require state-of-the-art systems integration (SI) capabilities with DevOps, and continuous integration and continuous deployment (CI/CD) processes. Few CSPs possess all these capabilities and must rely on a suitable vendor partner (or partners) to bridge the skills gap. In addition to strong SI capabilities, vendor partners must demonstrate key characteristics such as deep networking expertise, strong commitment to open-source solutions, compliance with industry standards and the ability to provide multi-vendor support.

2 The importance of network orchestration for CSPs

NFV and SDN technologies enable CSPs to apply cloud-based innovation approaches, automation tools and software-driven capabilities to the network, thereby offering next-generation digital services in an on-demand manner. The move away from the appliance-based networks to virtualised networking software on commercial hardware is one of two paths to realise automation. The other approach is to use SDN overlay technologies to achieve network automation in existing physical networks even as CSPs deploy native SDN-enabled networks. Using programmable software control, CSPs can significantly improve their business agility on multiple fronts including the speed of service innovation, reduced service deployment times and the ability to respond rapidly and flexibly to changing service demand. At the heart of this transformational change is the technology that provides this software control and programmability to the network – network orchestration (NO).

The analysis in this white paper is informed by an extensive primary research effort to understand the drivers, inhibitors and status of CSPs' network orchestrator implementations, their selection preferences and the challenges encountered during the implementation. The primary research consisted of 52 CSP surveys and 10 CSP interviews with CSPs from Asia–Pacific, Europe and North America, across all CSP tiers.[1] Survey participants provided answers to a series of closed-ended questions while the interviews entailed in-depth conversations with senior CSP executives whose titles ranged from VP in Network Engineering, President in Network and Service Operations to Head of Network Automation and OSS as well as Director in Network Transformation. All the participants for the primary research came from CSPs that are advanced in their thinking and deployment of network orchestrators. The analysis is also informed by Analysys Mason's continuous interviews with CSPs and other research in this field. .

2.1 The role and scope of network orchestration

Many large Tier 1 and Tier 2 CSPs have been on the NFV journey for between 5 and 7 years. The first step in the NFV evolution entails migrating the network functions out of the proprietary appliances onto commercial hardware and hosted on a hypervisor-enabled virtual machine on dedicated commercial hardware. From an operations perspective, the virtual network functions (VNFs) were treated much like the physical network function so did not require major changes except for

new considerations around managing the hypervisor-based virtualisation environment. However, as more VNFs were introduced into a common virtualisation environment, it quickly became apparent that CSPs could no longer rely on traditional network management systems (NMS) and manual processes for management and operations.

CSPs have also been implementing SDN-based technology to provide automation overlays or control plane extensions to existing control planes for their wide-area networks (WANs), comprising IP/optical access and transport networks. The first step in the WAN SDN journey relies on domain-specific controllers, based on either traditional NMS or its SDN-based evolution, in each individual domain. Subsequently, CSPs could plan to move onto a multi-layer WAN SDN control platform, which sits on top of separate domain-specific controllers to rationalise and simplify each silo with a horizonal, programmable management and control layer. In effect, it joins up network control and OSS-like lifecycle management functionalities. Due to the demands of high performance and near real-time network controls, the control layer needs to be implemented as a lightweight and independent module.

The existing network management and operations technology was conceived for physical networks with disparate operations support systems (OSS) leading to highly disjointed manual processes. CSPs have introduced incremental improvements over the years to improve efficiencies but the fundamentally different nature of the NFV/SDN-based networks, and the high levels of agility and operational efficiencies expected by the business mean that the current operations approach is not fit for purpose. CSPs need an operations approach based on automation, to configure and manage the lifecycle of VNFs and the virtualisation environment as well as to provision WAN-based connectivity. CSPs recognise that they need to do this at scale as they prepare for 5G and IoT with potential new agile B2B2X services. However, this will require an automation layer to rapidly stitch together and manage various network functions and domains as part of the end-to-end service. It is in this context that NO has emerged as a critical software function and a critical enabler of CSPs' network automation initiatives.

---

[1] Of the 52 CSPs surveyed, 7 were from North America, 23 were from Europe and 22 were from Asia–Pacific; 28 were Tier 1 and 2 CSPs, and 24 were Tier 3 and 4 CSPs. Of the 10 CSPs interviewed, 1 was from North America, 5 were from Europe and 4 were from Asia–Pacific; 8 were Tier 1 and 2 CSPs, and 2 were Tier 3 and 4 CSPs.

According to Analysys Mason, network orchestration consists of key software components to automate network operations.[2] Broadly, NO provides the ability to do three things: (a) automate the management of the lifecycle of the VNFs i.e., instantiation, placement, scale in/out, self-healing, upgrades, migration etc, (b) automate the provisioning and activation of service-specific network configurations to existing VNF instances or create new instances with the correct configuration; and (c) automatically set up connectivity in the WAN, either between VNFs or across physical equipment using SDN technologies. Figure 1 illustrates the key components and control lines of the NO: NFV orchestrator (NFVO), VNF managers (VNFM), and cross-domain network orchestrator (CD-NO). CD-NO manages an SDN controller that in turn manages connections between physical and virtual network functions.
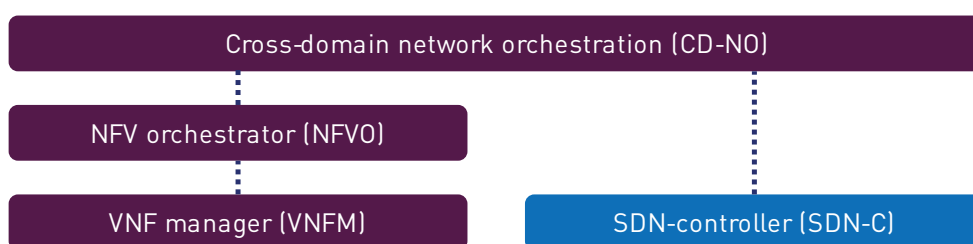

FIGURE 1: KEY COMPONENTS OF NETWORK ORCHESTRATION
[SOURCE: ANALYSYS MASON, 2019]

Based on research by Analysys Mason, CSPs are taking two distinct evolution paths for NO (see Figure 2):

• the 'NFV path' for the service lifecycle management and orchestration of VNFs

• the WAN SDN path' for software-defined control and automation of the WAN.

Ultimately, the two paths converge towards a fully integrated cross-domain orchestration system that not only orchestrates across networking domains[3] but also automates the functions of NFV lifecycle management and SDN control to create and provision services end-to-end by abstracting the underlying complexity. Even further down the road, cross-domain orchestration can extend to IT domains too.
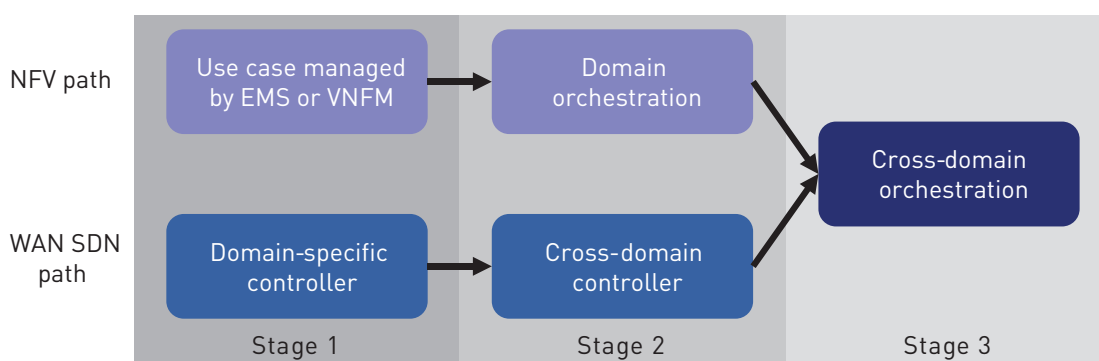
FIGURE 2: STAGES AND PATHS OF NETWORK ORCHESTRATION EVOLUTION
[SOURCE: ANALYSYS MASON, 2019]

[2] See Analysys Mason's Network automation and orchestration: worldwide forecast 2018–2022 (available at www.analysysmason.com/nao-forecast-rma07) for a detailed description of the functional blocks of NO.

[3] A domain may be associated with a specific technology, such as mobile connectivity or business services, or it could be geographically determined.

2.2 Motivations to deploy network orchestration

Figure 3 highlights the importance of network automation for CSPs. 75% of respondents thought of network automation as being at least a 'top-5' initiative, in fact 50% of CSPs considered network automation as a 'top-3' initiative in their company. CSPs from the Asia–Pacific region placed a particularly strong

emphasis on automation, with 82% of them assigning network automation as being at least a 'top-5' initiative, compared with around 70% of CSPs from Europe and North America. Tier 1 and 2 CSPs appeared to be more committed than smaller CSPs to network automation, with 82% of them considering it at least a 'top-5' initiative whereas the ratio among Tier 3 and 4 CSPs stands at 67%.
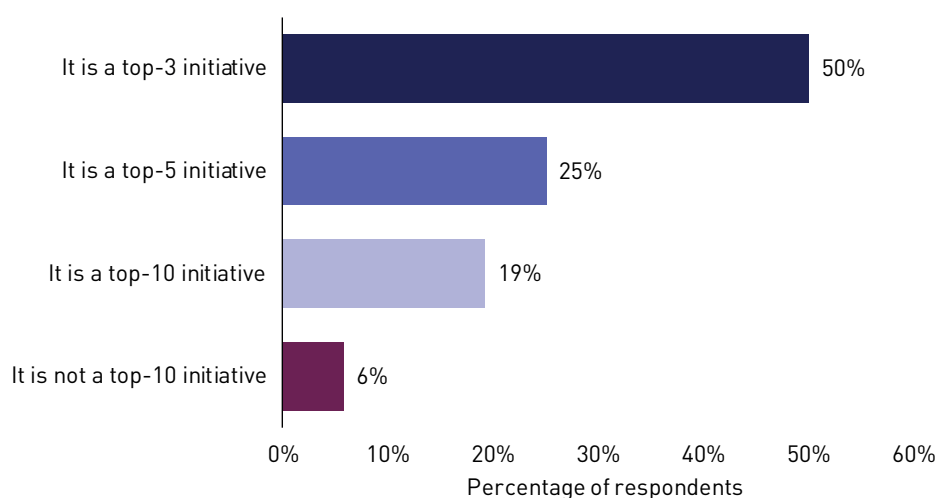
FIGURE 3: IMPORTANCE OF NETWORK AUTOMATION TO CSPS[4]
[SOURCE: ANALYSYS MASON, 2019]

Interviewed CSPs largely concurred with those we surveyed. Most of them observed a close link between 5G and network automation.

❝We have a huge, complex network consisting of fixed, broadband, television, mobile, data and enterprise solutions. As the entire telecoms industry is getting ready for the introduction of 5G, network virtualisation and automation is the need of the hour. On top of that we have more than 400 million mobile customers and we consider automation to be one of the top-three initiatives to enhance the customer experience.❞

Tier 1 multi-country CSP from Europe

❝We believe that 5G will provide a plethora of opportunities and the advent of 5G has been highly accelerated in the last three quarters, not only by OEMs but also by operators (to lead the 5G market) and governments (for example, those of Thailand and Malaysia). Considering the growing impetus for 5G, and the need for network slicing and more complex services, we need to prepare for deployment of orchestration and expect a shift toward orchestration pilots and initial deployment over the next 2–3 years.❞

Tier 1 single-country CSP from Asia–Pacific

---

[4] How important is increasing network automation overall to your company? [Select one answer only].

Service lifecycle management and network and service configuration automation stand out as the most popular motivation to deploy a network orchestrator, with well over half of surveyed CSPs considering them as the two most influential drivers (see Figure 4). Looking at CSPs from each region: 65% of European CSPs preferred *automating network and service configuration to service lifecycle management* (52% of European CSPs); but it was the opposite for APAC CSPs (55% and 68%, respectively); North American CSPs, while still leaning towards *service lifecycle management* also singled out *network complexity* as a significant factor; 71% of North American CSPs chose both as their main drivers for network orchestration.
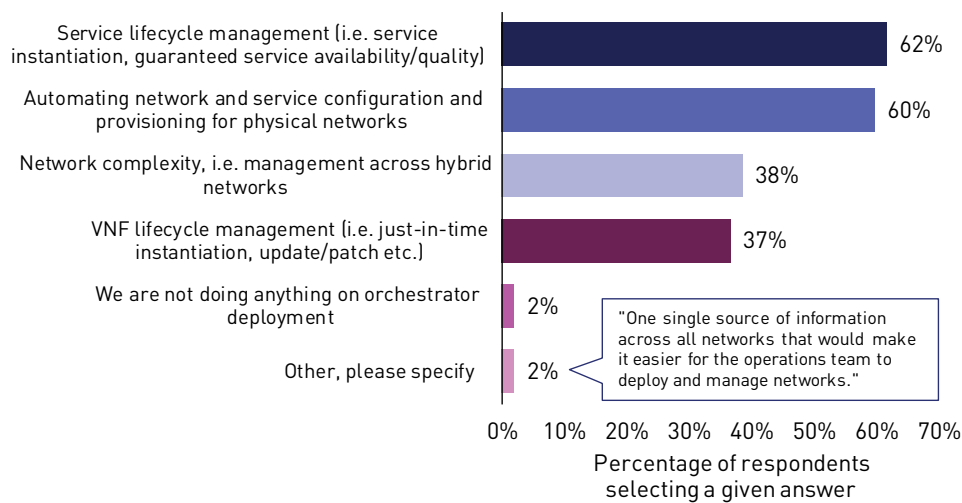
FIGURE 4: DRIVERS OF NETWORK ORCHESTRATOR DEPLOYMENT[5]
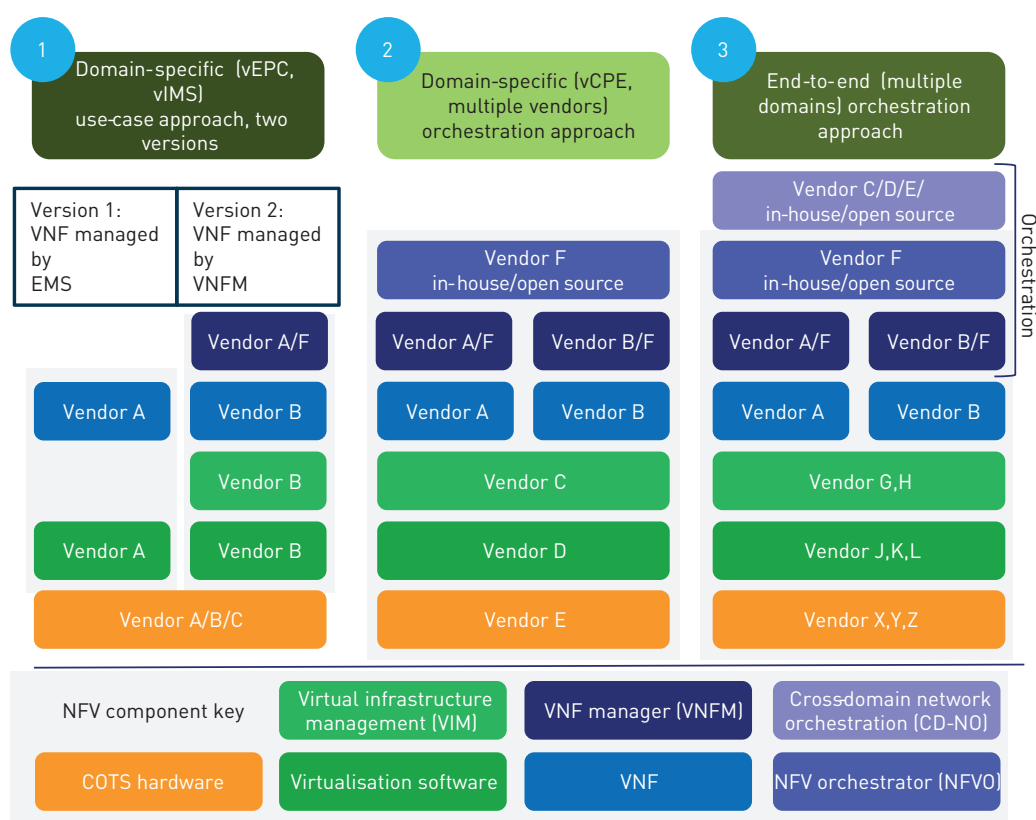[SOURCE: ANALYSYS MASON, 2019]

3 Overview of network orchestration deployments

The deployment approaches of network orchestration differ from CSP to CSP. Section 2.1 provided a high-level view of the two most prevalent paths – NFV path and the WAN SDN approach. This section will explore these two paths in more detail and discuss their deployment considerations, as well as highlighting the significance of professional services and systems integration services in enabling the journey towards the full end-to-end orchestration.

3.1 Architecture and deployment scenarios of network orchestrators in NFV and SDN

As CSPs make progress in NFV and WAN SDN deployments, scenarios are emerging that call for network orchestrators. Of the three deployment scenarios of NFV, network orchestrators are indispensable in the two scenarios that are more advanced (See Figure 5).

Pure NFV case. Not shown: orchestrator can also manage physical appliances

FIGURE 5: ORCHESTRATION IN NFV DEPLOYMENTS
[SOURCE: ANALYSYS MASON, 2019]

The most straightforward NFV deployment scenario that CSPs can undertake is by virtualising a single network function in a specific network domain. This is a relatively simple manoeuvre as it effectively creates a traditional network silo in a virtualised way using the existing management systems (with or without a VNFM) without the need for a network orchestrator (shown as NFVO in Figure 5). The VNF supplier is predominantly the party, oftentimes a NEP, that approaches the CSP with a pre-integrated solution.

As CSPs contemplate deploying a variety of VNFs on the same platform in a specific network domain,

domain specific network orchestrators are needed to support the operational automation and the onboarding and lifecycle management of individual VNFs. Leading CSPs are adopting end-to-end orchestration (shown as CD-NO in Figure 5) because of the need to manage a digital network and operations platform that extends across multiple network domains and combines NFV and SDN.

Advanced CSPs that began the automation and virtualisation journey earlier than the rest of the industry and have completed Scenario 1 in Figure 5 have already observed benefits, such as sizable cost

savings, more-efficient operations, improved service agility and resilience of virtualised networks. Some are looking forward to further benefits when orchestration kicks in.

The use of network orchestrators in WAN SDN

deployments (see Figure 6) is required when the CSP needs to automate across multiple SDN and NFV domains end-to-end. Before the final scenario, SDN controllers manage WAN components such as optical network components and IP routers with programmability and intelligence.
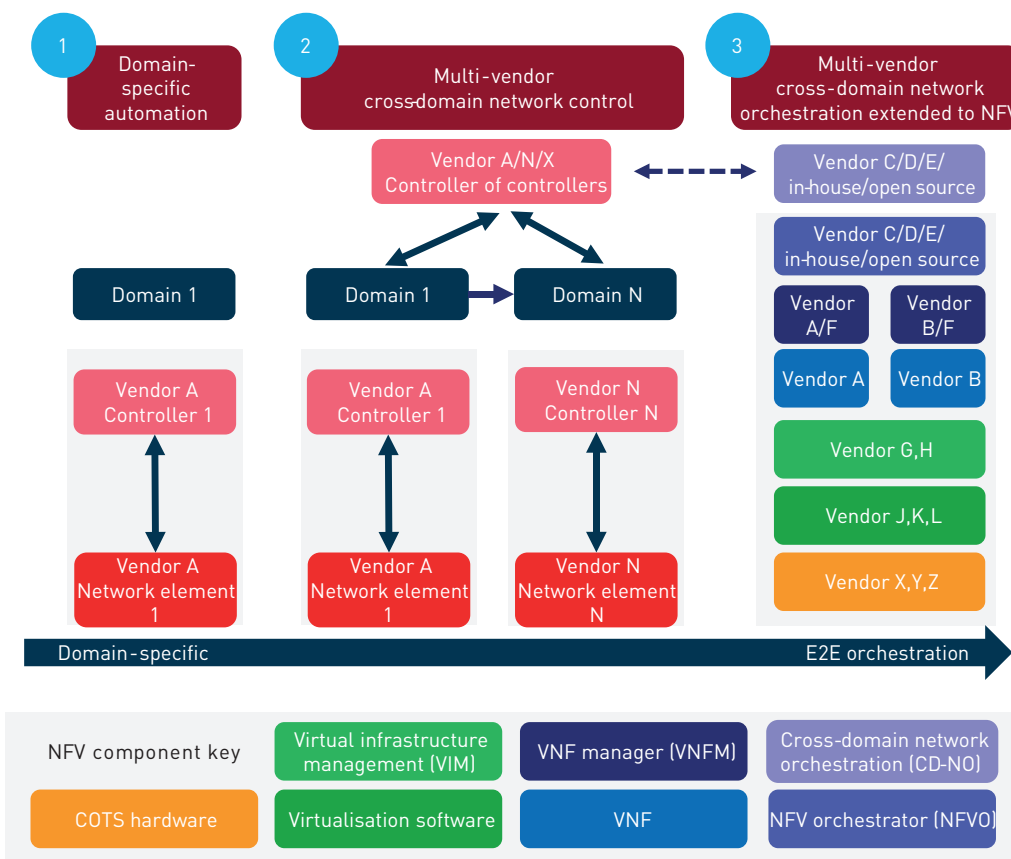
FIGURE 6: ORCEHSTRATION IN WAN SDN DEPLOYMENT
[SOURCE: ANALYSYS MASON, 2019]

CSPs can choose two paths in relation to WAN SDN deployment to obtain centralised and external control of the various WAN network elements, with trades-offs in terms of operational disruption, time to deployment and cost.

• CSPs can add an SDN layer on top of existing WAN infrastructure, without the need to remove and replace legacy infrastructure including optical and packet elements.

• Alternatively, or concurrently with the first path, CSPs need to have orchestration in place to deploy uCPE or vCPE, where the SDN-layer controls the virtualised CPE and NFVI is needed to host the WAN function as VNFs.

The journey to full end-to-end cross-domain orchestration is going to be incremental. CSPs will have a higher chance of success if they take a stepwise approach as illustrated in Figure 5 and Figure 6.

However, each of the stages will incrementally introduce new software components and new networking domains into the mix, which will require careful integration and validation before making the network orchestrators live. To reduce the risk of failure, CSPs will require robust systems integration capabilities that incorporate the latest software engineering principles such as DevOps and CI/CD.

Even in cases where CSPs procure commercial orchestration solutions, a significant level of customisation and systems integration will be required to make the solution suitable for their environments. Figure 7 illustrates such an architecture, in which the interplay of components is key, not necessarily the hierarchy on display.

Systems integration is needed to stich every domain together
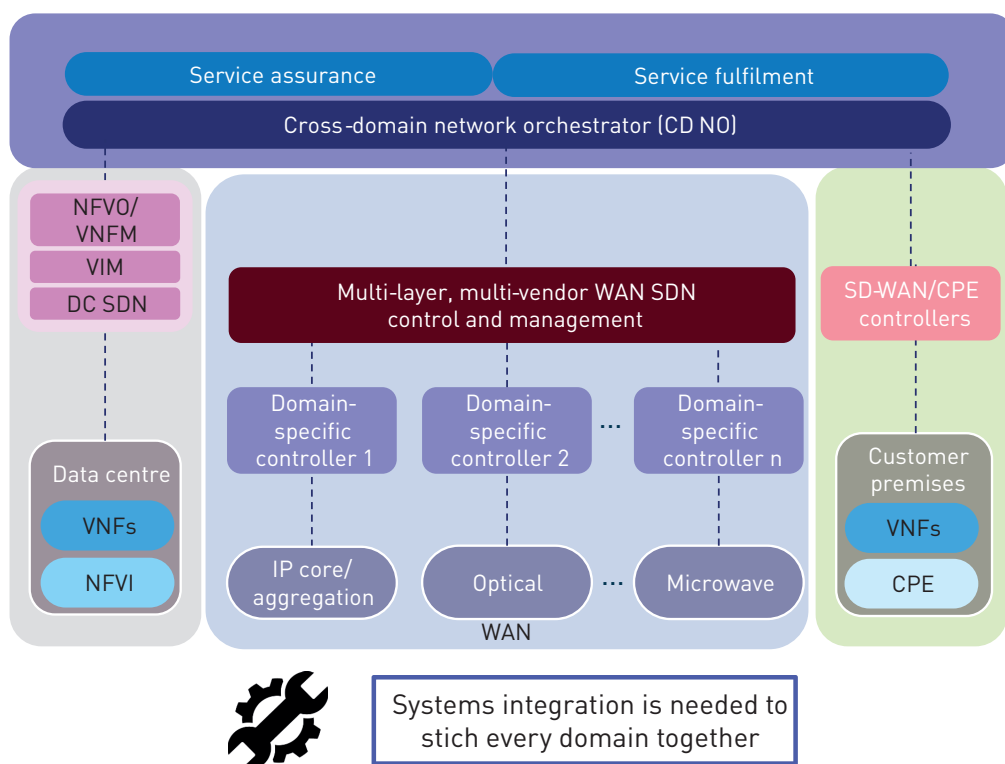
FIGURE 7: THE ROLE OF SYSTEMS INTEGRATION FOR NETWORK ORCHESTRATIONAUTOMATION
[SOURCE: ANALYSYS MASON, 2019]

3.2 Status of CSP network orchestrator deployment

Figure 8 illustrates the breakdown of orchestration approaches adopted by CSPs based on Analysys Mason's NFV/SDN contract tracker. As of 1Q 2019, 75% of NFV and SDN deployments are following the domain-specific approach that does not include any orchestration and 23% of these deployments have domain-specific orchestration in place, which went up from 14% of total deployments in 3Q 2017.

• The domain-specific use case approach entails individual VNFs implemented on their own dedicated NFVIs in a specific network domain. The VNF and NFVI can be managed by existing EMS/NMS/OSS with little, if any, orchestration. Deployments of vIMS and vEPC are prime examples of such an approach.

- A domain-specific orchestration approach enables CSPs to operate a platform on which multiple VNFs, from different vendors, are supported in a specific network domain. A prime example is vCPE, typically a part of a CSP's enterprise cloud.

- The end-to-end orchestration approach requires the CSP to commit to a cross-domain platform from the very start of its NFV activities. It builds on C-level commitment to NFV and strong corporate governance.
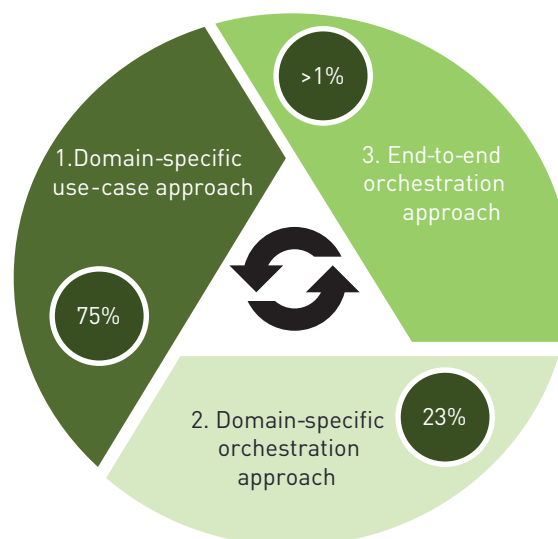
FIGURE 8: NFV/SDN DEPLOYMENT APPROACHES
[SOURCE: ANALYSYS MASON, 2019]

CSPs interviewed for this research have either deployed NFVO for specific domains or are still manging VNFs using VNFMs. End-to-end orchestration, due to its overwhelming impact on transition costs, staff training, legacy hardware and cross-domain expertise, has been considered only by the most advanced CSPs.

Currently, cross-domain orchestration is not in place and [orchestration] implementation is restricted to select domains within the company (e.g. the transport facility). Complete orchestration would require links between multiple databases to be dynamically and thoroughly established. For example, for anomaly detection, the company does not have a system in place for root-cause analysis or to take corrective actions.
Tier 1 multi-country CSP from Europe

NFVO has been deployed for the IMS core. We are considering the use of NFVO for SD-WAN as well. Our first NO phase focused on the lifecycle management of networks, primarily via the automation of network administration tasks. We have created a framework with our existing vendors regarding the implementation of NO. This includes an internal database creation of existing licenses to avoid overpaying for the same VNF and thus keeping the costs in control. Currently, plans to integrate all the different network orchestrators into a single common layer of service orchestration are being considered.
Tier 1 single-country CSP from North America

We have yet to deploy a network orchestrator as we currently rely on VNFM. We plan to use VNFM until maturity before deploying a network orchestrator.
Tier 1 multi-country CSP from Europe

4 Customer expectations from an orchestration solution

CSPs need to offer their network services across digital channels, whenever they want, wherever they want. CSPs foresee the use of network orchestrators to help them deliver such a user experience by composing highly-curated products and services on demand and delivering them to the customers in a matter of minutes. This section introduces the findings from CSP interviews on what benefits they expect network orchestrators to bring about and the survey results on prioritised use cases enabled by NFV orchestration and WAN automation.

CSPs interviewed for this research largely echoed the same motivations from survey respondents for the deployment of network orchestrators (see Figure 4), namely:

• enabling service lifecycle management

• enabling VNF lifecycle management

• automating network and service configuration and provisioning for physical networks

• managing network complexity.

In terms of VNF and service lifecycle management, CSPs agreed that network orchestrators would help to ease the management of the network through a single source of information and support differentiated service quality so as to secure customer loyalty. Some cautioned that VNF lifecycle management has yet to work well with large-scale deployment. Others called out 5G and the associated enterprise opportunities as a key trigger to resort to network orchestrators.

A combined OSS and NFVO provides a single source of information. This makes it easier for the network management team to deploy, operate and manage the network. It is also easier to manage end-to-end life cycle of VNFs as the operations team has a single source to understand how the network is performing.
Tier 1 single-country CSP from Asia–Pacific

Service lifecycle management is an important revenue driver as it will enable a high quality of service, which will prove to be an important differentiator in the consumer experience thus ensuring loyalty. However, even though vendors advertise the efficiency of the scale in and scale out functions, in reality the functions don't work efficiently at large-scale deployments.
Tier 1 single-country CSP from Asia Pacific

We believe that 5G will provide enterprise business opportunities (such as healthcare and automated card services and undertaking network slicing). Therefore, to avail these opportunities, an aggregator would need to have configuration mechanisms that enable shorter lead time. The life cycle management service is important here owing to its capacity to configure and deploy a service faster. It also segregates the service on the basis of quality delivery.
Tier 1 single-country CSP from Asia–Pacific

From the perspective of automating networks and servicing configuration and provisioning of networks, reduction of human errors, reduced time to market and more efficient network investment are well recognised benefits that CSPs expect to realise from network orchestrator deployment. Traffic lifecycle management is further down the road.

We are working to reduce the downtime caused due to human error, expediting new service delivery. Orchestration also helps cut down operational costs significantly and improves productivity by automating labour-intensive tasks, thus increasing reliability by decreasing human error rates.
Tier 1 multi-country CSP from Europe

The data demand surges would be accommodated via the dynamic allocation of existing hardware. This would lead to a reduction of manual forecasts and planning functions within the operations department, which would facilitate further cost savings. It would also improve investment efficiency, because advanced investment in capex needed for physical deployments would be avoided.
Tier 1 single-country CSP from Europe

Traffic lifecycle management is the next step of evolution. The IMS, EPC, and other core network functions will need to be configured onto a common platform to achieve the same.
Tier 1 single-country CSP from Asia–Pacific

Against the backdrop of increasing network complexity, CSPs are looking to network orchestrators as a single source of information with visibility across domains and as an enabler for a single customer account across various networks.

“ *As we offer a wide range of services for various networks (consisting of fixed, broadband, mobile, data and enterprise solutions), it is extremely important for the company to offer personalisation and create a single account (across all networks) for customers to access and manage these services.* ”

Tier 1 single-country CSP from Asia–Pacific

“ *Orchestration provides visibility of various network components as one single source of information across all networks that would make it easier for the operations team to deploy and manage networks.* ”

Tier 1 single-country CSP from Asia–Pacific

Figure 9 presents the top-2 use cases enabled by NFV orchestration and WAN automation from surveyed CSPs. One in four considered *vEPC* as a high-priority use case. Indeed, it was consistently recognised as the most important use case more times than any other use case among various segmentations of surveyed CSPs except among Tier 3 and 4 CSPs, which instead assigned greater priority to *multi-vendor device/service configuration*. Half of APAC and Tier 1 and 2 CSPs (50% in both groups), considered *vEPC* as one of the two most important use cases. European CSPs have a wider distribution of top-2 use cases with *vEPC* and *vIMS* (both 30% of European CSPs) slightly ahead of *multi-vendor device/service configuration and multi-layer control for IP/optical domain* (both 26% of European CSPs).
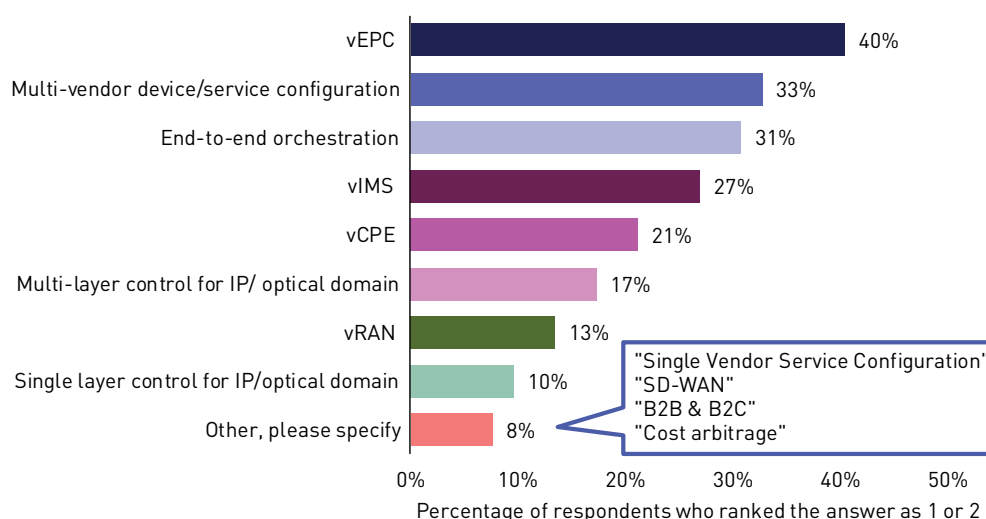
FIGURE 9: PRIORITISED USE CASES FOR NETWORK ORCHESTRATION AND WAN AUTOMATION[6]
[SOURCE: ANALYSYS MASON, 2019]

---

[6] What are the prioritised use cases enabled by NFV orchestration and WAN automation? [Rank the following options in terms of importance: 1 being most important, 5 being least important]

5 Deployment options and challenges

This section presents the results and analysis of the survey questions and interview discussions pertaining to the challenges and considerations for deploying network orchestrators at scale, ranging from network orchestrator procurement approaches and preference of network orchestrator suppliers to attitude to open source and challenges associated with deploying orchestrators at scale.

5.1 CSPs' network orchestrator procurement strategies

CSPs can take many approaches to implement the NO but most are likely to adopt some sort of a hybrid approach depending on their risk appetite, availability of in-house technological expertise and the senior-level executive commitment to the cause. Historically when faced with a similar decision, CSPs have chosen either:

- to build the technology themselves with some external vendor support around application development and systems integration
- to buy a commercial off-the-shelf software from vendors specialising in that area of telecoms software, with an expectation that the vendor will provide a certain level of product support and maintenance over time.

The survey showed that 40% of the CSPs surveyed were planning to co-develop the network orchestrator with a vendor partner. This is not surprising given how important NO is for business success, and therefore CSPs would like to retain some level of knowledge and expertise within the company.
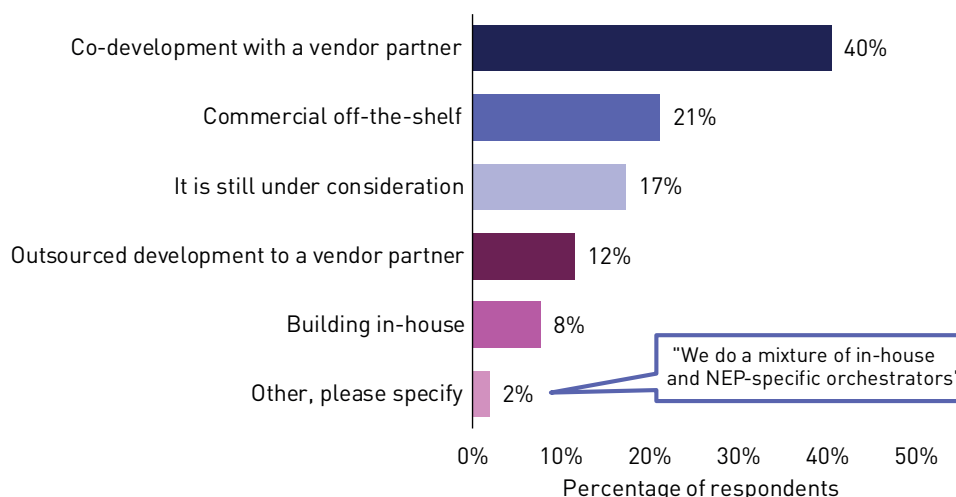
FIGURE 10: CSPs BUILD VERSUS BUY STRATEGY FOR NETWORK ORCHESTRATORS[7]
[SOURCE: ANALYSYS MASON, 2019]

The co-development process helps to retain some key knowledge within the organisation. As the system evolves, rather than relying on a single vendor, the company undertakes joint projects with multiple vendor partners for different tasks.

Tier 1 multi-country CSP from Europe

It is quite clear that most CSPs do not have all the expertise in-house to develop the technology entirely on their own and are therefore opting for a combination of approaches for different components of the network orchestrator; for example, procuring a commercial NFVO product with varying degrees of customisations to suit the operations, while also considering the option of using select open-source components from ONAP and enhancing the functionality using internal capabilities.

---

[7] What is your build vs. buy strategy for orchestration solutions? [Select one answer only]

On the other hand, 21% of the respondents said that they would prefer a commercial network orchestrator solution from a vendor because they did not have the capability to build the solutions in-house but also valued the deep domain expertise and knowledge, and experience in building and implementing products. Furthermore, such CSPs often work to an aggressive plan to commercialise NFV/SDN so the quickest way for them to commercialise a solution is to procure the solution from a vendor.

Looking into specific segmentation of surveys CSPs, those in APAC are more likely to opt for *commercial*

off-the-shelf solution (36% of CSPs in APAC) rather than co-development (32% of CSPs in APAC). It is noteworthy that 21% of Tier 3 and 4 CSPs considered it viable the option of *outsourcing development to a vendor partner*, relative to 12% of all surveyed CSPs.

5.2 CSPs' preferences for network orchestrator vendor partners

The survey revealed that 76% of the CSPs showed a clear preference for NEPs as one of the top-2 suppliers of network orchestrators, followed by OSS vendors and SIs.
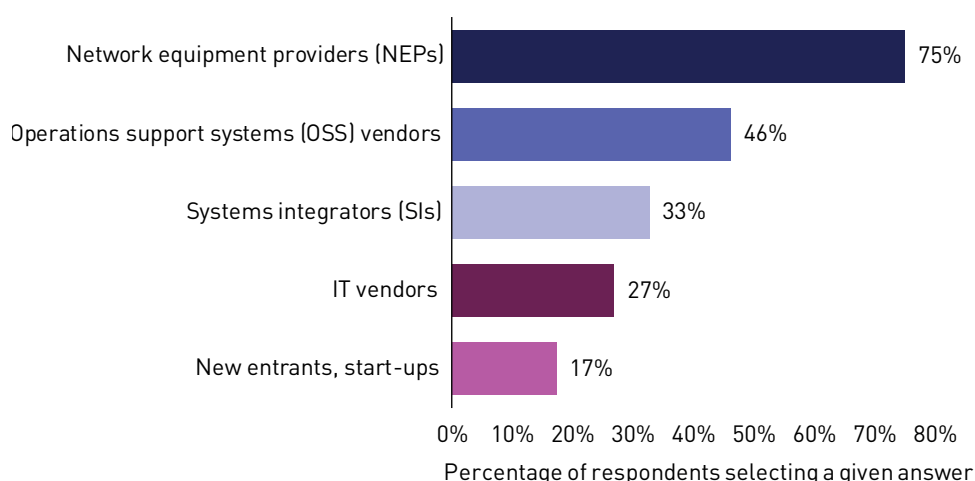
FIGURE 11: PREFERRED SUPPLIERS OF NETWORK ORCHESTRATORS[8]
[SOURCE: ANALYSYS MASON, 2019]

CSPs that chose NEPs as their first choice attributed their preference to:

- the deep domain knowledge of the NEPs

- the fact that the NEPs are rapidly migrating to software-led businesses

- a long history of operating telecoms networks

- understanding of the NFV- and SDN-related performance requirements

- the ability to overcome customisation difficulties for complex networks.

The NEPs possess a high degree of domain knowledge. They have a good understanding of the KPIs related to NFV for wireless network functions, making them an ideal fit for the role of network orchestrator suppliers.
Tier 1 single-country CSP from Europe

Some CSPs preferred OSS suppliers over NEPs as their preferred partner because those CSPs thought of the network orchestrator as an enhanced version of the OSS. As such, OSS vendors have a better understanding of the orchestration requirements and can act as an independent option that is not necessarily tied to the underlying VNFs or NFV infrastructure.

While the option of new entrants is the least popular one, selected by 17% of surveyed CSPs, Tier 1 and 2 CSPs appeared relatively more courageous to take a chance with them on these (21% of tier 1 and 2 CSPs) compared with 13% among Tier 3 and 4 CSPs.

For CSPs that preferred the co-development with vendor partners, they were also more willing, compared with the overall respondent base, to take risks by enrolling the help of new entrants and start-ups (29% compared with 17%). By contrast, 82% of CSPs that indicated a stronger reliance on vendors, i.e. preferring COTS and outsourced solutions, have a clear preference for NEPs as their ideal supplier of network orchestrators.

### 5.3 CSPs' attitudes towards open-source solutions

The survey revealed that 71% of the CSPs demonstrated a clear commitment to using open-source technologies for network orchestrators, while only a small minority (6%) said that they do not prefer open-source solutions (see Figure 12).

It was also evident that many CSPs would prefer to use

a vendor partner either to supply the open source software or a vendor customised distribution of the open source software – over half of the CSPs (55%) preferred this approach. This shows that the CSPs are not entirely confident of executing the open source strategy on their own, mainly owing to two broad issues:

- reliability: large-scale open-source deployments have a propensity to develop a higher level of operational issues compared to proprietary software
- support: large-scale deployments require significant organisation commitment in terms of engineering and operations support, which may not always be available in-house.

None of the North American CSPs explicitly expressed their dislike of open-source solutions, while featuring the greatest percentage of CSPs (43% of North American CSPs) that were still reviewing their open-source strategies. All three CSPs that explicitly did not like open-source systems are Tier 3 and 4 CSPs.
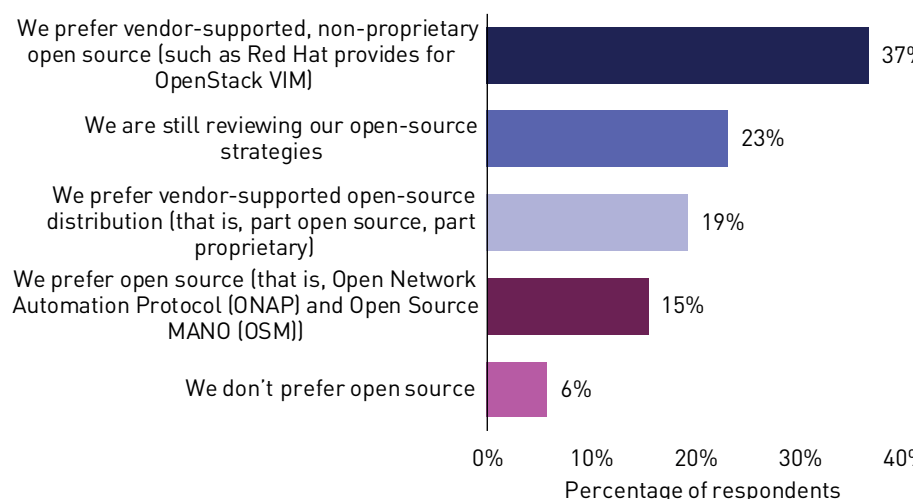
FIGURE 12: ATTITUDE TO OPEN-SOURCE SOLUTIONS[9]
[SOURCE: ANALYSYS MASON, 2019]

❝ For nationwide deployments of orchestration solutions, big support teams are needed. We have already deployed over 4000 servers for NFV systems, and thus need a big support team for software troubleshooting. Our vendor partner is providing the support team, which helps to reduce the costs.

The open-source software is attractive but can only be operationally feasible if an operator has an in-house development team for the same. However, many operators find it difficult to develop and maintain such teams. ❞
*Tier 1 single-country CSP from Europe*

5.4 Top-4 challenges for CSPs to deploy network orchestrators at scale

CSPs face multiple technology and organisational challenges that impede on the pace of network orchestrator deployment. Figure 13 shows that the most prominent four choices were: lack of technology maturity, lack of the right skillsets, change management and the need for high levels of customisation.

- **Lack of technology maturity:** the lack of standards and clear specifications for network orchestrator has led to diverse product implementations in the commercial vendor space and competing solutions in the open-source arena, creating fragmentation and market confusion. Consequently, there has been slow progress on maturing the technology for mass deployment.

- **Lack of right skillsets:** skillsets of engineering and operations personal are still largely network-centric, whereas the demands of NFV, SDN and cloud require a more software and automation centric skills. CSPs

need to therefore reskill their existing staff and/or hire new staff with the requisite skills to succeed in this transformation.

- **Need for customisation:** even the commercial orchestration products cannot be quickly operationalised because each CSP has different multiple vendor systems operating within the same environment. Additionally, the interoperability of VNFs across different domains is a challenge as the VNFs would be configured as per the vendor's own network orchestrator implementation.

- **Change management:** the success of orchestration depends on the success of broader organisational change. Changing people's mindsets away from the traditional manual operations to automation-first mindset is going to be pivotal. Furthermore, the change management processes that were designed for the legacy manual operations must be reimagined to suit network orchestrator-based automation.
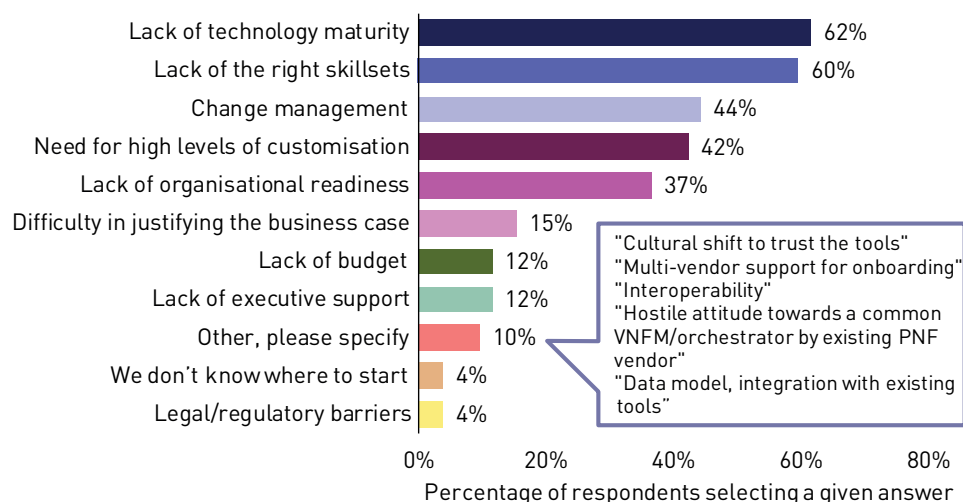
FIGURE 13: CHALLENGES OF DEPLOYING NETWORK ORCHESTRATORS[10]
[SOURCE: ANALYSYS MASON, 2019]

6 CSP expectations of good network orchestrator vendor partners

The network orchestration space is competitive with various vendor groups such as NEPs, OSS/ orchestration vendors, and new-entrant ISVs making a play for business; open-source platforms have also emerged as a viable alternative, which are being productised by some vendors and/or being incorporated within commercial solutions. However, very few CSPs can realise the vision of full orchestration without significant external support. CSPs need a 'partner' for their orchestration journey,

be it in enabling them to make sensible buy/build decisions or co-developing fit for purpose commercial/ custom/open source-based solutions for the CSP's unique requirements or offering a build–operate– transfer model.

Based on research by Analysys Mason on the topic of network orchestration and the insights generated from primary research for this study, we have summarised the key characteristics that CSPs associate with good network orchestrator vendors.

CHARACTERISTIC	DESCRIPTION
Demonstrate deep networking expertise	CSPs view favourably those vendors that have a deep expertise in networking with R&D resources and understanding of the networks and operations, especially where they are incumbent.
Possess strong systems integration and professional services proposition (or via partners)	Network orchestration systems will require high levels of customisation to make them suitable for the CSP. Systems integration capabilities will be required to operationalise the orchestration system within the CSP's automation platform and ecosystem.
Show strong commitment to open-source solutions	Vendors must clearly articulate their open-source strategy and demonstrate a clear roadmap of how they plan to incorporate open-source modules in their orchestration solutions or comply with open-source initiatives such as ONAP and OSM. CSPs also value vendors' contribution to open-source communities and initiatives to tap open source where applicable.
Comply with standards	Orchestration vendors must demonstrate standards compliance and actively participate in industry-wide initiatives. The solutions must support standard data modelling languages such as NETCONF/YANG/TOSCA, and comply with industry specifications developed by MEF, TMF, IETF, ETSI and ONF etc.
Build open platforms	Orchestration solutions must be open and easy to integrate into cross-domain network orchestrator (CD-NO), adjunct domain controller and other higher layer operational systems through open northbound and southbound interfaces/APIs. The solutions must also support larger ecosystems with open APIs and SDKs for the developer community.
Enable incremental deployment	Vendors should offer a flexible deployment approach to enable CSPs to start with either the NFV path or WAN SDN path for limited domains/services and expand to multiple services/domains over time.
Demonstrate capabilities in cloud native development, DevOps and CI/CD	Vendors should embrace the cloud-based software engineering practices such as microservices based architecture and common software libraries, and DevOps and CI/CD for operations-led rapid software development. These approaches enable rapid onboarding of new functions to meet future requirements.
Provide multi-vendor support	CSPs expect the network orchestrator to support multi-vendor VNF environment with the ability to easily onboard new VNFs and vendors; therefore, it is imperative that the vendor solutions support multi-vendor VNFs by design.
Incorporate machine learning and AI capabilities	CSPs are increasingly demanding ML and AI capabilities in operations. Orchestration solutions that use ML/AI can make just-in-time decisions and predictions for various use cases such as scale-in/scale-out, self-healing and closed-loop assurance.
Participate in industry and partner ecosystems	CSPs prefer vendors that demonstrate their commitment to ecosystems because this shows the vendor's willingness to collaborate and co-develop solutions and bring in specialised partners for best-of-breed implementations.
Flexible commercial model	Vendors must not only innovate in technology but also provide innovative commercial models in addition to the traditional licensing approaches. CSPs are increasingly demanding usage-based, pay-as-you-grow, SaaS and success-based models.

FIGURE 14: CSPS' EXPECTATIONS FROM GOOD NETWORK ORCHESTRATOR VENDOR PARTNERS
[SOURCE: ANALYSYS MASON, 2019]

7 Conclusions and recommendations

Network orchestration plays a pivotal role in the operationalisation and automation of NFV- and SDN-based networks. CSPs are following two distinct paths to achieve their automation goals, one led by the network virtualisation and service lifecycle management, and the second for software-driven control and automation of the WAN. Ultimately, these paths converge with the implementation of the end-to-end cross-domain network orchestration system that will provide end-to-end control of various network orchestration and SDN control systems.

CSPs must carefully consider the path towards full end-to-end orchestration and make suitable choices for the network orchestration technology. The technology must demonstrate various traits such as the ability to provide automated VNF and service lifecycle management, automating network and service configuration and provisioning for physical networks, and provide necessary levels of abstraction to manage network complexity. In parallel, CSPs can pursue automation in the WAN by deploying SDN control technology in existing physical networks even as they pursue native SDN components in the network.

The journey to end-to-end orchestration is going to be incremental and will demand another level of skills and resource commitment from CSPs. However, most CSPs will find it daunting to execute the initiatives all by themselves and will need a vendor to support them through this journey. CSPs will expect to partner with a vendor that aligns with their orchestration strategy and will want to co-develop the orchestration technology with their vendor partner, and in some cases entirely outsource the development to the partner.

Vendors must demonstrate a multitude of capabilities to be chosen as a preferred partner for network orchestration. CSPs favour vendors that possess deep networking expertise, strong systems integration and professional services capabilities, and show a strong commitment to open source technology. Vendors must also prove their credibility in providing multi-vendor support and cloud-based software development approaches such as DevOps and CI/CD.

About the authors

Anil Rao (Principal Analyst) is the lead analyst for Analysys Mason's *Automated Assurance* and *Service Design and Orchestration* research programmes, covering a broad range of topics on the existing and new-age operational systems that will power telcos' digital transformation. His main areas of focus include: service creation, provisioning, and service operations in NFV/SDN-based networks, 5G, IoT, and edge clouds; the use of analytics, ML and AI to increase operations efficiency and agility; and the broader imperatives around operations automation and zero-touch networks. In addition to producing quantitative and qualitative research for both programmes, Anil also works with clients on a range of consulting engagements such as strategy assessment and advisory, market sizing, competitive analysis and market positioning, and marketing support through thought-leadership collateral. Anil is also a frequent speaker and chair at industry events, and holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

Hansang (Andy) He (Consultant, Custom Research) works in Analysys Mason's Custom Research team. He has worked on engagements commissioned by a range of clients, ranging from telecoms operators and industry bodies to quasi-autonomous non-governmental organisations and vendors. Much of his recent work has focused on network virtualisation and digital transformation, encompassing case studies underpinned by quantitative business models, vendor evaluations, competitive landscape studies and development of go-to-market strategies. He began his career as an analyst covering the emerging Asia–Pacific (EMAP) region. Andy holds a bachelor's degree in Electronic and Communications Engineering from the University of Bristol and a master's degree in Management and Strategy from the London School of Economics and Political Science.

This whitepaper was commissioned by Fujitsu. Analysys Mason does not endorse any of the vendor's products or services.

Analysys Mason's consulting and research are uniquely positioned

Analysys Mason is a trusted adviser on telecoms, technology and media. We work with our clients, including CSPs, regulators and end users to:

- design winning strategies that deliver measurable results

- make informed decisions based on market intelligence and analytical rigour

- develop innovative propositions to gain competitive advantage.

We have around 265 staff in 16 offices and are respected worldwide for the exceptional quality of our work, as well as our independence and flexibility in responding to client needs. For over 30 years, we have been helping clients in more than 110 countries to maximise their opportunities.

Consulting

- We deliver tangible benefits to clients across the telecoms industry:
  - communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers.

- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.

- We are future-focused and help clients understand the challenges and opportunities that new technology brings.

Research

- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.

- We offer detailed insight into the software, infrastructure and technology delivering those services.

- Clients benefit from regular and timely intelligence, and direct access to analysts.
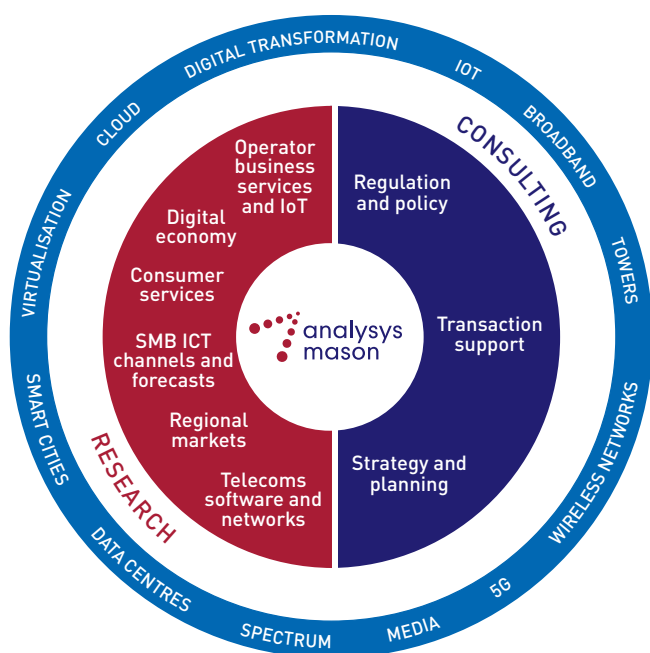
Research from Analysys Mason

We provide dedicated coverage of developments in the telecoms, media and technology (TMT) sectors, through a range of research programmes that focus on different services and regions of the world

The division consists of a specialised team of analysts, who provide dedicated coverage of TMT issues and trends. Our experts understand not only the complexities of the TMT sectors, but the unique challenges of companies, regulators and other stakeholders operating in such a dynamic industry.

Our subscription research programmes cover the following key areas.

Consumer services programmes
Mobile Services
Mobile Devices
Fixed Broadband Services
Convergence Strategies
Video Strategies

Operator investment programmes
Operator Investment Strategies
Network Traffic
Spectrum

Telecoms software and networks programmes
Software Forecast and Strategy
Telecoms Software Market Shares
Network-focused
Next-Generation Wireless Networks
Video and Identity Platforms
Service Design and Orchestration
Automated Assurance
Network Automation and Orchestration
Digital Infrastructure Strategies
Customer-focused
Digital Experience
Customer Engagement
Monetisation Platforms
AI and Analytics

Digital economy programmes
Digital Economy Strategies
Future Comms

Operator business services and IoT programmes
Large Enterprise Voice and Data Connectivity
Large Enterprise Emerging Service Opportunities
SME Strategies
IoT and M2M Services
IoT Platforms and Technology

SMB ICT channels and forecasts programmes
Managed Service Provider Strategies
Cyber Security

Regional markets programmes
Global Telecoms Data
Americas
Asia–Pacific
Middle East and Africa
European Core Forecasts
European Telecoms Market Matrix
European Country Reports

DataHub
~2500 forecast and 250+ historical metrics
Regional results and worldwide totals
Operator historical data

Each subscription programme provides a combination of quantitative deliverables, including access to more than 3 million consumer and industry data points, as well as research articles and reports on emerging trends drawn from our library of research and consulting work.

Our custom research service offers in-depth, tailored analysis that addresses specific issues to meet your exact requirements

Alongside our standardised suite of research programmes, Analysys Mason's Custom Research team undertakes specialised, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customised industry intelligence and insights.

For more information about our research services, please visit www.analysysmason.com/research.

Consulting from Analysys Mason

For more than 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities

Our clients in the telecoms, media and technology (TMT) sectors operate in dynamic markets where change is constant. We help shape their understanding of the future so they can thrive in these demanding conditions. To do that, we have developed rigorous methodologies that deliver real results for clients around the world.

Our focus is exclusively on TMT. We advise clients on regulatory matters, help shape spectrum policy and develop spectrum strategy, support multi-billion dollar investments, advise on operational performance and develop new business strategies. Such projects result in a depth of knowledge and a range of expertise that sets us apart.

REGULATION AND POLICY

- Policy development and response
- Ex-ante market reviews, remedies, costing ...
- Universal Service Obligation (USO)
- Scarce resources: radio spectrum management, auction support, numbering ...
- Ex-post/abuse of dominance
- Postal sector

TRANSACTION SUPPORT

- Commercial due diligence
- Technical due diligence
- Mergers and acquisitions (M&As)
- Debt and initial public offerings (IPOs)
- Joint-venture structuring
- Mid-market financial sponsors

STRATEGY AND PLANNING

- Commercial expertise
- Technology optimisation
- New digital frontiers

analysysmason.com/consulting

We look beyond the obvious to understand a situation from a client's perspective. Most importantly, we never forget that the point of consultancy is to provide appropriate and practical solutions. We help clients solve their most pressing problems, enabling them to go farther, faster and achieve their commercial objectives.

For more information about our consulting services, please visit www.analysysmason.com/consulting.

Stay connected

You can stay connected by following Analysys Mason
via Twitter, LinkedIn, YouTube or RSS feed.

@AnalysysMason

linkedin.com/company/analysys-mason

youtube.com/AnalysysMason

analysysmason.com/RSS/

analysysmason.podbean.com