Perspective

Multi-vendor network management: bridging legacy and 5G networks

October 2021

Anil Rao and Andrew Killeen

Contents

List of figures

1. Executive summary

Communication service providers (CSPs) have traditionally used expensive and proprietary networking solutions that are built for purpose, and new solutions and applications are often integrated discretely over time. Further, digital transformation and network disaggregation have fuelled CSPs' approach towards multi-vendor networks. This shift away from expensive and proprietary networks offers greater control and flexibility, and allows the CSP to select from best-of-breed products and applications.

However, the legacy element and network management solutions have been built as closed systems, designed to exclusively manage a vendor's own networking products services and solutions, and require custom integrations with a higher-layer OSS. This proprietary management layer creates individual vendor silos, increases the total cost of ownership (TCO) of the network, and makes 5G network economics unsustainable in the long term.

A multi-vendor, unified network management architecture enabled by software-defined networking (SDN) simplifies operations and paves the way for 5G. CSPs can achieve opex and capex efficiencies by combining management systems, consequently reducing the network TCO. Fujitsu's online calculator can calculate the TCO of any network based on the user's parameters.[1] This report includes the results for a hypothetical network configuration operating in the present mode of operation (PMO) and future mode of operation (FMO) over a 10-year period. This hypothetical network configuration maintains 150 000 network elements covered by seven element management systems (EMSs) in the PMO compared to a single, consolidated network management system (NMS) in the FMO. Fujitsu's calculator estimates that the consolidated NMS and operational improvements reduce the TCO by 33% and can improve energy efficiency by 30%.

SDN control capabilities enable a higher level of network automation, granular resource control and programmability, which can provide further operational benefits. Such a platform also enables CSPs to go one step further towards offering differentiated, customisable, and on-demand network-as-a-service solutions and delivering the services in an agile and scalable manner. The SDN controllers across the multi-vendor network management architecture must comply with open APIs for CSPs to rationalise their existing management silos without having to rip and replace infrastructure. Equally, the new architecture will need to fulfil many requirements, such as support for both legacy and next-generation networks, unified network topology, telemetry and ML/AI capabilities, and model-driven network abstraction, for CSPs to achieve their digital transformation objectives.

However, most CSPs do not have the relevant in-house resources and expertise to implement such a unified platform and must rely on a suitable technology partner. CSPs need a partner that can manage and deliver all aspects of the implementation (such as consulting, custom development and systems integration), while complying with the latest software engineering paradigms such as container and microservices-based development for cloud deployment, and agile principles, such as DevOps and CI/CD pipelines.

[1] Available at: https://www.fujitsu.com/us/products/network/solutions/ems-consolidation/index.html.

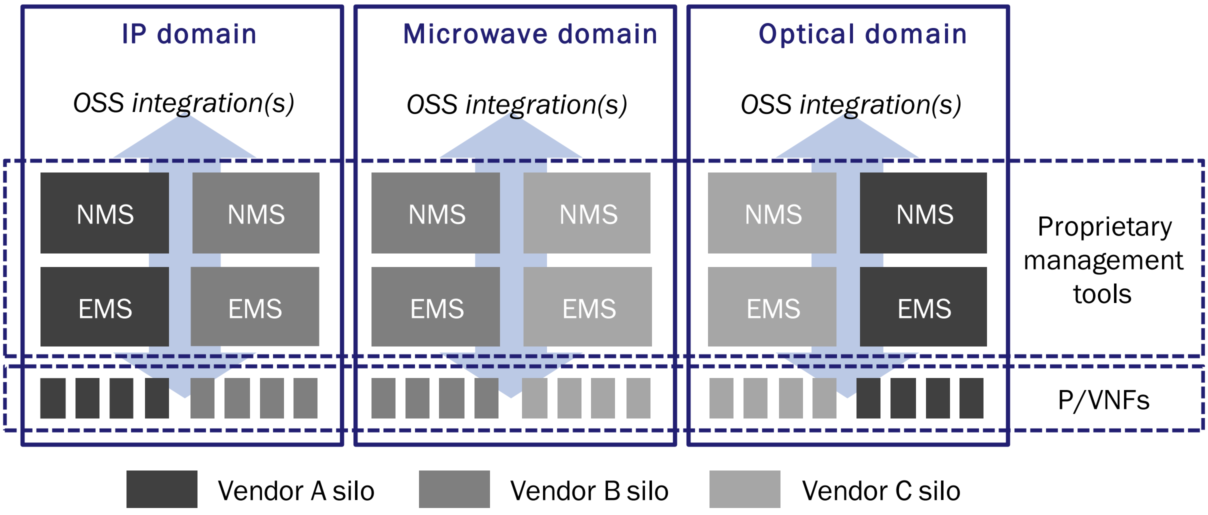
2. CSPs are forced to deal with proprietary network management systems and siloed operations

CSPs have traditionally used expensive and proprietary networking solutions built for purpose, which has resulted in CSPs relying on a single vendor to operate and maintain their networks. New solutions and applications are deployed discretely over time, resulting in complex and siloed operations. The resulting network is a build up of vendor-specific NMSs, device-type-specific EMSs and domain-specific interfaces, often for specific verticals or domains.

CSP digital transformation projects have heavily featured network disaggregation across network domains, from the core, edge, and transport networks. Network disaggregation decouples the network hardware and software to deploy cloud-native, software-driven networks that emulate the operational efficiencies achieved by hyperscalers and cloud providers. The key drivers for this transformation, among others, is to reduce the TCO of networks and to foster innovation. CSPs want to capitalise on new operating models and multi-vendor strategies that allow it to select and deploy the best-of-breed networking solutions. Network disaggregation makes it easier for CSPs to move away from the traditional operating model and take a multi-vendor strategy that offers more options, control, and flexibility for CSPs to select best-of-breed products and applications.

Figure 1 shows an example of a disaggregated network where the CSP has selected different vendors for different solutions and deployed best of breed physical and virtual network functions (P/VNFs) across network domains. Many vendors continue to build their applications without open APIs that require the vendor's own EMSs and NMSs, creating a layer of proprietary management tools made up of individual vendor silos. Each silo will then need to be integrated with the CSP's OSS and will typically result in domain-specific interfaces (for example, CORBA, SNMP, MTOSI, XML, FTP, REST, CLI).

Figure 1: Example of management silos across network domains and different vendors' solutions



Source: Analysys Mason, 2021

The proprietary management layer, requiring individual, discrete integrations and interfaces has slowed the progress of CSPs' digital transformation, despite their ability to select from best-of-breed solutions. Without open standards, most vendor tools and processes will not interoperate by default in a multi-vendor environment or with the CSPs' higher-layer control and management.

This approach to a multi-vendor strategy using traditional integration methods has created serious and expensive long-term problems. Network engineering and operations departments typically develop manual processes to work around interoperability issues but require extensive internal and external staff to manage the massive sprawl of integrations, leading to ever-increasing software integration and maintenance costs. Each integration may be independently optimised to shorten the time to revenue and improve service fulfilment processes for the specific domain. However, these integrations often rely on inefficient, manual actions for service design, activation and assurance, and CSPs must simultaneously make significant changes to the OSS, which limits CSPs' ability to offer new services in a timely manner. As this becomes the standard operating procedure, undocumented operations and knowledge solidify, making future change and transformation more challenging.

As CSPs pursue a multi-vendor strategy, the list of management systems and domain-specific interfaces will continue to grow and hamper the CSPs' digital transformation. Most Tier-1 CSPs already deal with many management systems, specialist operations teams, and vendor-specific integrations and interfaces. This scale of vendor-specific integrations, each with its own proprietary management system, adds significant overhead to the CSPs' operations and maintenance, and introduces extreme complexity for integrating new solutions.

New next-generation 5G networks will increasingly use cloud-native, virtual, and software-driven components as CSPs look for new revenue opportunities, automation-led cost transformation and service differentiation. However, today's networks will probably continue to operate for the foreseeable future. The long-term operations of these legacy networks that rely on proprietary management tools and manual processes will become unsustainable and hamper CSPs' plans for next-generation networks.

To avoid repeating past mistakes and deploying new operational silos, CSPs will need a new approach for multi-vendor network management, easing the integration and maintenance challenges of the existing networks while preparing for the 5G era.

3. Multi-vendor network management reduces TCO and prepares CSPs for 5G

The transport network domain provides immediate opportunities for CSPs to consolidate their management layer and move away from the siloed management tools. The principles for managing a multi-vendor network will remain applicable to other networking domains, and the scope of abstraction can be extended further to create a multi-layer, multi-vendor SDN architecture.

3.1 Domain-specific unified management platforms provide a scalable blueprint architecture

A modern unified network management platform provides the core capabilities to manage the lifecycle of physical and virtual network functions, resources and services within that domain. The platform can then be powered with SDN capabilities and open APIs to enable programmability and openness to serve as an abstraction layer between the OSS and each of the vendor silos underneath. This will allow a simple approach for future integrations of new solutions and decouple the OSS from the network, enabling both the OSS and the network to evolve independently and at a reasonable pace without incurring additional integration and operational overheads. This domain-based unified management approach can then be scaled up to cover multiple transport network domains and vendor silos.

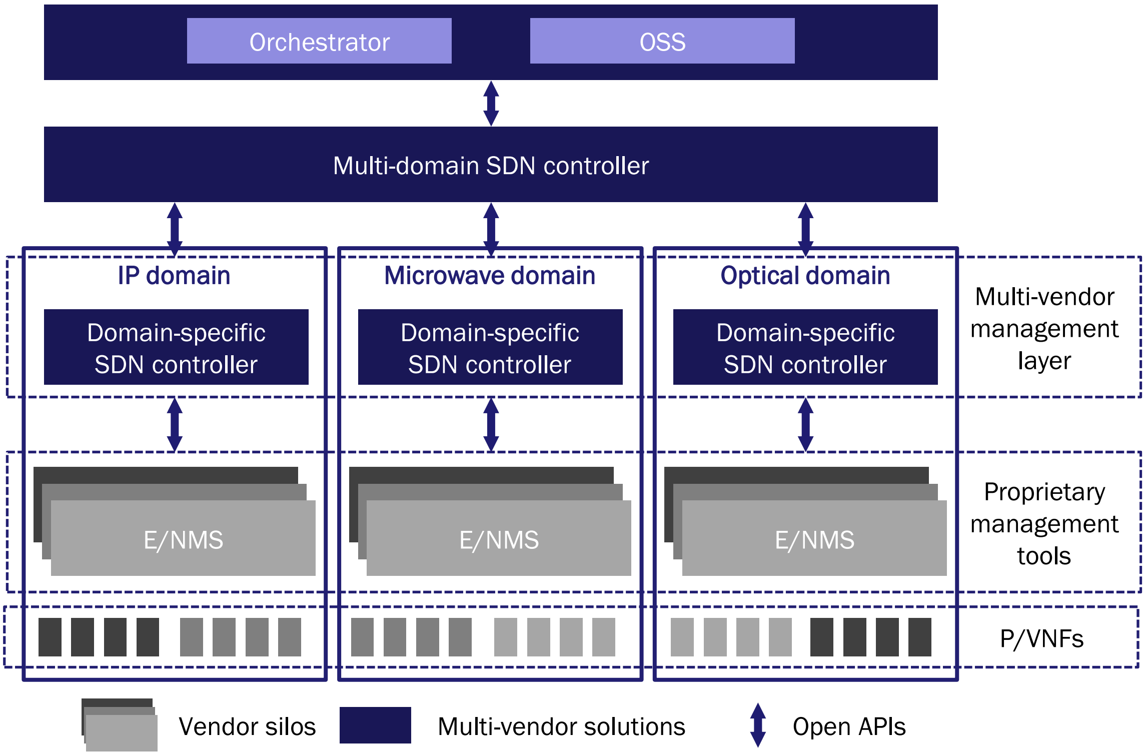
Figure 2 shows an example of a hierarchical approach to network management in a multi-vendor, multi-domain environment. The result is a common management architecture that gives CSPs the flexibility to pursue a unified management approach and a multi-vendor strategy.

- The higher-layer, multi-domain SDN control platform provides an abstraction layer to the OSS for control and management functions of each transport network domain (for example, IP, microwave and optical). The multi-domain SDN controller may then use standardised APIs to interact with each domain level unified management platform.

- Each transport domain features a unified domain-level management platform with SDN capabilities that interacts via standardised APIs with the vendor-specific network and element management systems.

- The lower layer then includes vendor-specific elements and network management systems where the CSP has integrated best-of-breed solutions from different technology vendors.

Figure 2: Example of a hierarchical multi-vendor, SDN-based network management architecture for the transport network


Orchestrator
OSS
Multi-domain SDN controller
IP domain
Microwave domain
Optical domain
Domain-specific SDN controller
Domain-specific SDN controller
Domain-specific SDN controller
Multi-vendor management layer
E/NMS
E/NMS
E/NMS
Proprietary management tools
P/VNFs
Vendor silos
Multi-vendor solutions
Open APIs

Source: Analysys Mason, 2021

This example network uses open APIs to provide end-to-end and centralised management and control of multiple network domains. Each domain-specific management layer rationalises the proprietary management tools from different vendor silos. The multi-domain SDN controller provides an abstraction and operational demarcation in a highly distributed network architecture including the various transport networks.

The foundational capability of the solution is to provide multi-domain control and multi-vendor control at different layers and allow for network programmability. Such a solution will allow CSPs to significantly reduce the network TCO and offer differentiated, customisable enterprise services on-demand and operate in a faster, more-automated way with an agile approach to service delivery (that is, creation, activation, modification, and termination).

3.2 A unified network management layer can deliver benefits to CSPs

A multi-layer network management solution provides a more-centralised, abstracted, and multi-vendor management plane for the network, and is a natural evolution from the disparate NMSs and EMSs. The common management and control plane from such a solution can benefit CSPs in many ways.

- Achieve greater opex and capex efficiency by using a combined operations and management system, with less of an operational overhead compared to managing multiple silos. Further efficiencies come from decoupling the OSS and network, allowing for simple integration when deploying new solutions.

- Take advantage of extreme automation and network programmability, paving the path to autonomous networks and network slicing. Greater automation and programmability will improve service agility, reduce time-to-revenue, and improve operational efficiency.

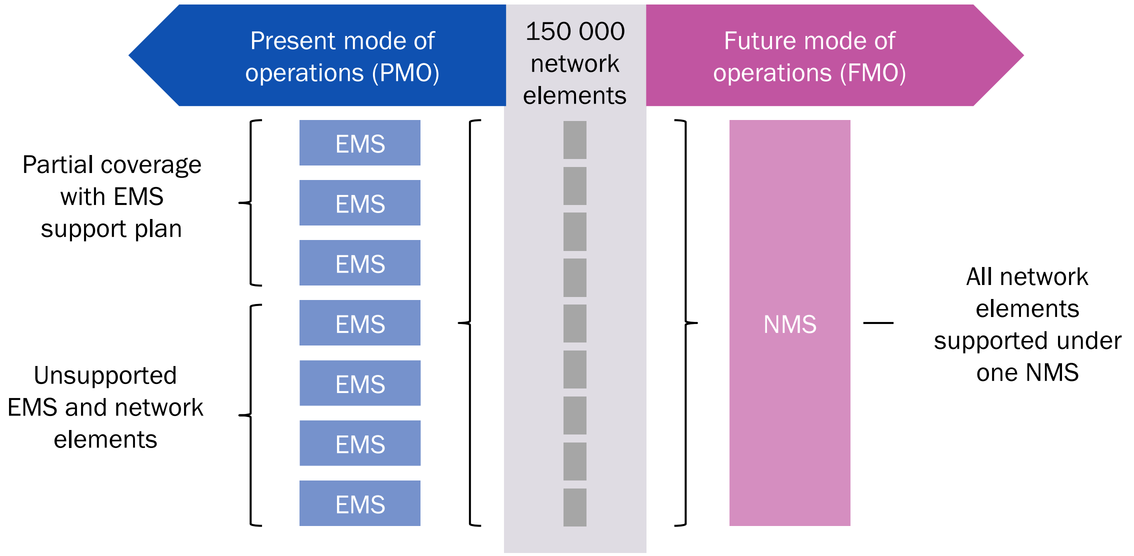
- Deploy future-proof technology and prepare for 5G and next-generation networks by collapsing the separate control planes and legacy EMS and NMS architecture. This will allow for information sharing and analytics across network domains and between the new next-generation networks and todays' existing networks.

- Reduce dependency on a single vendor and allow CSPs to benefit from vendor competition and select the best-of-breed solutions that comply with their architecture.

An abstracted, multi-domain network management layer will also enable new business models such as network-as-a-service (NaaS). Much like the software-as-a-service (SaaS) model that has disrupted IT products, CSPs will be able to deliver highly dynamic and customisable services to enterprises. By exposing the physical and virtual network resources and capabilities to a service catalogue, the new abstract layer can programmatically control and manage the network to meet enterprise customers' needs and SLAs. The level of automation required for the NaaS model will enable CSPs to dynamically compose new services and automate the lifecycle management.

Fujitsu has developed a TCO model to quantify the benefits of migrating to a multi-vendor NMS solution.

Figure 3: Overview of the network configuration considered in the PMO and FMO for Fujitsu's TCO calculation


Present mode of operations (PMO)
150 000 network elements
Future mode of operations (FMO)
Partial coverage with EMS support plan
Unsupported EMS and network elements
EMS
EMS
EMS
EMS
EMS
EMS
EMS
NMS
All network elements supported under one NMS

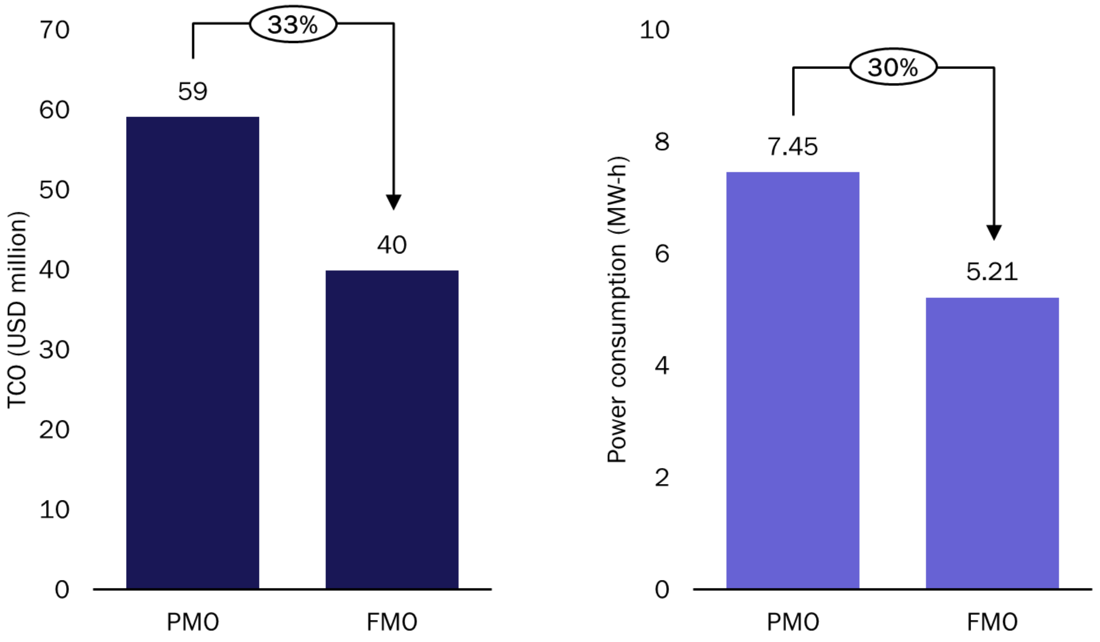
Source: Fujitsu Network Communications, 2021

Fujitsu's TCO calculator assumes a hypothetical network configuration and assesses the costs of the PMO and FMO over 10 years. Figure 3 shows how the hypothetical network configuration maintaining 150 000 network elements differs between the PMO and FMO. In the PMO, all network elements are covered by seven EMSs, of which three EMSs and 95 000 network elements are under the EMS support plan; the remaining EMSs and network elements are unsupported. For the FMO, one supported NMS covers all network elements. Further assumptions are detailed in section 6.1.

Figure 4 shows the benefits estimated by Fujitsu's TCO calculator comparing the costs modelled to their hypothetical network configuration between the PMO and FMO. Fujitsu's calculator estimates:

- a reduction in the TCO by 33% owing to the transition from seven EMSs to a consolidated NMS
- a reduction in power consumption costs by 30% owing to the transition from large, old, power-hungry specialised servers to efficient, compact and operationally simplified servers.

Figure 4: Benefits to the TCO and power consumption estimated by Fujitsu's TCO calculator



Source: Fujitsu Network Communications, 2021

Disclaimer: Fujitsu's estimated benefits are based on typical assumptions[2], the actual network configuration and results will vary for different CSPs.

3.3 Fast-evolving open standards are making it easier to unify the network management layer

The disaggregation of optical and IP networks is accelerating the introduction of open APIs. Open APIs will enable CSPs to avoid vendor lock-in, improve their ability to manage network complexity and lay the groundwork for disaggregated, software-driven networks that will be required for 5G.

TIP's Open Optical & Packet Transport (OOPT) project group is working to standardise the open transport SDN architecture, starting with technical specifications for the northbound and southbound APIs for common CSP use cases. The project group is backed by several major Tier-1 CSPs, such as Deutsche Telekom, Orange, Telefónica, Telia Company and Vodafone, among others, that are looking to achieve vendor-agnostic network

[2] Users may enter their own parameters to Fujitsu's TCO calculator at: https://www.fujitsu.com/us/products/network/solutions/ems-consolidation/index.html.

control and management. The OOPT project group recently demonstrated end-to-end service operations and network visibility across an open, partially disaggregated and multi-vendor optical network.[3]

Maturing standards using open APIs enable CSPs to deploy highly interoperable networks and operational systems, paving the way for a multi-vendor network management layer. Open APIs are essential for the rapid development and production of new products and services at scale. Several standards already exist for the telecoms industry:

- RESTCONF, developed by the Internet Engineering Task Force (IETF), or OpenConfig can be used for the northbound API for the domain controller of IP networks

- NETCONF/YANG can provide the data model for the microwave domain controller

- OpenConfig along with NETCONF/YANG can be used as the information model for the optical network domain controller.

The OOPT collaboration, led by several major Tier-1 CSPs is an important step towards the goal of a vendor-agnostic, standards-based programmable network that can be highly automated and provide 5G network slices.

[3] Telecom Infra Project (2021), demonstration of the management and control of an open network. Available at: https://telecominfraproject.com/tip-oopt-project-group-completes-successful-proof-of-concept-open-optical-networks/.

4. CSPs must consider a set of factors and capabilities for their multi-vendor network management solution

4.1 The multi-vendor network management solution must provide some essential capabilities

Compliance with open, industry-standardised APIs is the key capability for unified network management that will rationalise the network management silos and allow CSPs to use their existing investments without ripping and replacing existing infrastructure. However, the unified management solutions must simultaneously support the management and control of legacy and next-generation 5G networks. Figure 5 summarises other capabilities that CSPs should expect from a unified network management system.

Figure 5: Key characteristics of a unified network management system

Platform requirement	Description
Support for legacy and next-generation networks	A future-proof common architecture that can automate the legacy physical resources and virtual network functions, and the next-generation, open, disaggregated networks.
Multi-vendor planning and design	Automated control and configuration of the physical and virtual resources and applications, and the corresponding management systems, in a multi-vendor environment.
Unified fault and alarms management	Rapid policy-based network assurance functions (for example, traffic re-routing) that are vendor-agnostic and network-aware.
Automated network discovery and inventory	Capable of real-time or near real-time computation of the network resources and traffic paths across network domains and different vendors' solutions, and able to serve plug-and-play functionality for new third-party or open-source applications or resources.
Unified network topology	A real-time, single source of the network topology with visibility, resource pooling, advanced monitoring, predictive analytics and control across all layers and domains. An automated source of the network topology prevents human errors and increases data accuracy, allowing data to be automatically consumed for service fulfilment and assurance.
Telemetry and ML/AI	Data extraction of the network telemetry from multi-vendor solutions across the network layers and domains. The telemetry data will then be essential to implement the extreme automation of network control and management functions. Open access to the telemetry can then use ML/AI algorithms to implement advanced use cases, such as traffic steering, to improve resource utilisation, reduce congestion and guarantee the delivery of differentiated SLAs.
Security	Tightly integrated and distributed security from core to the edge is inherent to cloud-native technologies, delivering reliable security for the converged network and end-to-end services that run over it.
Model-driven network abstraction	Provide an abstraction layer between the OSS and the components of the underlying network domains and vendor solutions. This will be essential to offer NaaS with a high level of customisation for different, bespoke enterprise requirements.
Multi-vendor service provisioning	Vendor-agnostic service lifecycle management, capable of orchestrating all the exposed network applications and resources from different vendors to provision, manage and control services on-demand.
Virtual network function (VNF) lifecycle management and orchestration	VNFs will be able to autonomously consume network data with a high level of confidence. These functions will then be able to programmatically trigger lifecycle management and orchestration processes, improving productivity and reducing the time to provision these services, in turn reducing the time to revenue for the CSP.

Source: Analysys Mason, 2021

4.2 CSPs must consider several factors when choosing a technology partner to implement the unified network management solution

Many CSPs lack the in-house resource and expertise to manage the transformation process, integrating disaggregated components, operations and service lifecycle processes, and complex value chain management, required to deploy a unified network management system. CSPs must also consider a set of key factors when choosing a technology partner for unified network management system.

- The technology should be built using cloud-native and microservices principles that support DevOps and CI/CD pipelines to automate the build, test and deployment processes. This will prevent 'tool sprawl' and new management silos from emerging, while increasing the automation efficiency of solution development and deployment.

- Using modern software development approaches, such as DevOps and CI/CD pipelines, the partner should be able to rapidly onboard new features and functions to cover additional services and network domains and deliver the future business requirements. This should also simplify the management and backwards compatibility of legacy services for the existing infrastructure.

- The partner should use a platform-based approach with a modular architecture using microservices that will enable CSPs to easily integrate new capabilities and develop new network functions and features with minimal disruption to the OSS and ongoing business operations. The partner should then be able to swap modules in a plug-and-play fashion depending on the CSP's needs.

- The partner should provide business and design consulting, custom development and systems integration to manage and deliver all aspects of the project, including solution integration and migration, requirements gathering and specification, and process and workflow design, among other project types. The partner should also support various deployment models for different modules or solutions, such as on-premises and cloud software, or SaaS.

5. Conclusions

- **A multi-vendor network management architecture simplifies operations and paves the way for 5G.** A modern multi-vendor unified network management solution powered by SDN control capabilities can deliver significant benefits to CSPs. This SDN-based abstraction layer significantly simplifies the network management of CSPs' networks allowing them to implement a hierarchical, SDN-based control architecture, which will enable programmatic network control and extreme automation across the network domains and vendor silos. This architectural approach will support CSPs' digital transformation objectives to reduce the TCO of operating the existing networks while also setting a strong foundation for efficiently operating future 5G networks. Fujitsu's own TCO calculations based on a hypothetical network estimates a reduction of 33% over a 10-year period by using a consolidated NMS to manage a multi-vendor network environment.

- **Compliance with open, industry-standardised APIs is key to implementing the unified network management solution.** Open APIs are essential for the rapid development and deployment of new products and services at scale. Further common solution capabilities from a unified network management system include support for legacy and next-generation networks, unified network topology, telemetry and ML/AI capabilities, and model-driven network abstraction.

- **CSPs need a suitable technology partner to implement the new management and control architecture.** Most CSPs lack the necessary in-house, technical expertise and skillsets required to implement the new architecture. The partner should offer DevOps personnel and use CI/CD pipelines to automate the build, test and deployment processes, and rapidly onboard new features and functions. For the new architecture to be future ready, the partner must then adhere to using microservices and cloud-native, modular components. Further, the partner should support the CSP with business and design consulting skills, custom development, and systems integration to deliver all aspects of the project.

6. Fujitsu's NMS consolidation

The Fujitsu EMS Transformation solution helps CSPs to keep legacy assets in service while reducing security risks and recurring opex. The Fujitsu multi-vendor solution uses a microservices-based architecture and containerised secure micro applications, laying the foundation for a flexible network that is positioned to take advantage of network intelligence and advanced automation.

Modular, open and secure

With open and standard APIs, CSPs may apply any or all of Fujitsu's network automation micro applications to southbound connections using TL1, SNMP and NetConf. Fujitsu micro applications deliver specific automated network control and management across vendors, domains, layers and systems, delivering unified management from a modernised system.

These micro applications are delivered within a containerised, microservice-enabled framework that is scalable, available, modularised and secure. New network elements and solutions from other vendors can be easily added and integrated.

Start with the basics and deploy additional capabilities as needed

CSPs with large legacy networks can take a phased approach to EMS transformation, beginning by replacing a handful of outdated element management systems, and mapping legacy EMS retirement to digital infrastructure deployment.

CSPs can start with basic network element functionality:

- back up, restore and upgrade
- network equipment (NE) maintenance – smart terminal ('reach through')
- local alarm management
- local performance management.

CSPs can then extend basic NE management to include unified management:

- SDN control and management
- component integration
- discovery
- topology
- NE database, organisation and nesting
- scheduling
- reporting
- craft tool.

Built for value

A fully functional flexible network operations model can scale in minutes rather than months with rules-based automated scaling, to quickly increase or decrease capacity per application or function based on traffic demands. Fully optimised hardware resources with advanced automation that ties incremental hardware investment to customer satisfaction rather than technology availability.

The Fujitsu flexible network operations model

Micro applications, advanced network analytics and intelligence-driven automation enable CSPs to drive efficiencies throughout network operations as they replace and consolidate their management systems. The EMS

Transformation Solution is part of the Fujitsu unified multi-layer, multi-vendor network stack. These products are members of the Fujitsu hybrid CT/IT infrastructure family, expanding the reach, productivity and value of the communications network.

6.1 Fujitsu TCO model assumptions

Fujitsu's calculations include the management system licence and support costs, network operating costs, and potential costs from outages and security breaches.

- The software licence and support costs in the PMO includes the cost of the maintenance and support plan for network elements. Many network elements may be managed by EMSs that are not covered by this maintenance and support plan. In the FMO, these costs reflect the CSP's initial investment in the consolidated NMS and the support plan for subsequent years.

- The volume and growth of network equipment maintained in the network and operating costs for the EMSs will vary by network. These operating costs consist of server power consumption, the physical space required, and support personnel.

- Unsupported EMSs in the PMO are less reliable and more likely to result in network downtime or outages. By supporting all network elements with the consolidated NMS, the network in the FMO is more reliable and avoids potential downtime.

- Unsupported EMSs in the PMO are more vulnerable to security breaches. By supporting all network elements with the consolidated NMS, the network in the FMO is more secure, reducing the risk and potential costs associated with network security breaches.

7. About the authors

Anil Rao (Research Director) is the lead analyst on network and service automation research that includes the *Network Automation and Orchestration*, *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 operators' digital transformations. 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. 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.

Andrew Killeen (Consultant) has worked with a wide range of clients worldwide, including network operators, vendors and industry bodies. His work focuses on using market analysis, sizing and forecasting, and competitive benchmarking to inform clients' planning and strategy. His project experience has ranged from 5G and the internet of things to virtualisation, cloud technologies and machine learning. Much of Andrew's work has used original, international research, including expert interviews and consumer and enterprise surveys.

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

Analysys Mason Limited. Registered in England and Wales with company number 05177472. Registered office: North West Wing Bush House, Aldwych, London, England, WC2B 4PJ.

We have used reasonable care and skill to prepare this publication and are not responsible for any errors or omissions, or for the results obtained from the use of this publication. The opinions expressed are those of the authors only. All information is provided "as is", with no guarantee of completeness or accuracy, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will we be liable to you or any third party for any decision made or action taken in reliance on the information, including but not limited to investment decisions, or for any loss (including consequential, special or similar losses), even if advised of the possibility of such losses.