WHITE PAPER

FROM AUTONOMOUS TO ADAPTIVE: THE NEXT EVOLUTION IN NETWORKING

Gorkem Yigit and Dana Cooperson

FEBRUARY 2018

analysysmason.com

Contents

List of figures

1. Executive summary

Recent developments and progress in automation and artificial intelligence (AI) technologies are generating significant interest and investments in many industries; information and communication technologies (ICT) is no different. Network providers are now able to rethink their operations with AI to achieve their long-desired goal of end-to-end automation, but most of them do not want to cede control to networks that decide their own direction and remove humans from the equation altogether. Most network providers want their networks and operations to become more 'adaptive' to respond to an ever-changing competitive landscape and consumer demands, which requires a coherent combination of human-controlled and -supervised automated operational processes, analytics-driven intelligence, and an underlying programmable infrastructure.

This white paper aims to set a clear vision for the future 'adaptive' wide-area transport networks and their operations. It provides a definition of an adaptive network and discusses the key market and operational forces that are driving network providers to make their networks more adaptive. It describes the key building block components of adaptive networks and provides an overview of the key requirements that providers should be looking for when procuring these solutions/components. The paper then analyses the potential migration paths that providers can take to adaptive networks and recommends a stepwise approach to building adaptive networks without the need for a major transformation. It also discusses several use cases for adaptive networks and provides a real implementation case example from a network provider (Windstream). Finally, it provides best practices for network providers to overcome the technological, operational and organizational challenges for building adaptive networks.

2. Moving beyond the autonomous network to the adaptive network

The ICT world has undergone many disruptive changes in the last decade. The rapid adoption of smartphones created a new digital economy driven by mobile applications and services that empower business and consumer customers alike. The availability of fixed broadband and the proliferation of on-demand streaming services such as Netflix have revolutionized the traditional TV/video industry. Similarly, cloud computing has upended enterprise IT strategies and pushed new, high-capacity connectivity requirements as business applications and workloads increasingly move to public cloud services (SaaS/IaaS) and cloud data centers.

These new technologies and services continuously reshape user behavior, expectations and demand. This is disrupting the existing market dynamics, and creating new market opportunities and emerging players that are threatening the legacy organizations, which cannot keep up with the rapid change. In such a rapidly changing environment, as in nature, the winners are not going to be those that are the most powerful or clever, but those that are the fittest: those that can adapt to the changes quickly and effectively.

Network providers today are faced with this challenge of adapting to the constantly evolving ICT landscape; they need to achieve more agile and lean operations that are underpinned by an 'adaptive network'.

2.1 What constitutes an adaptive network?

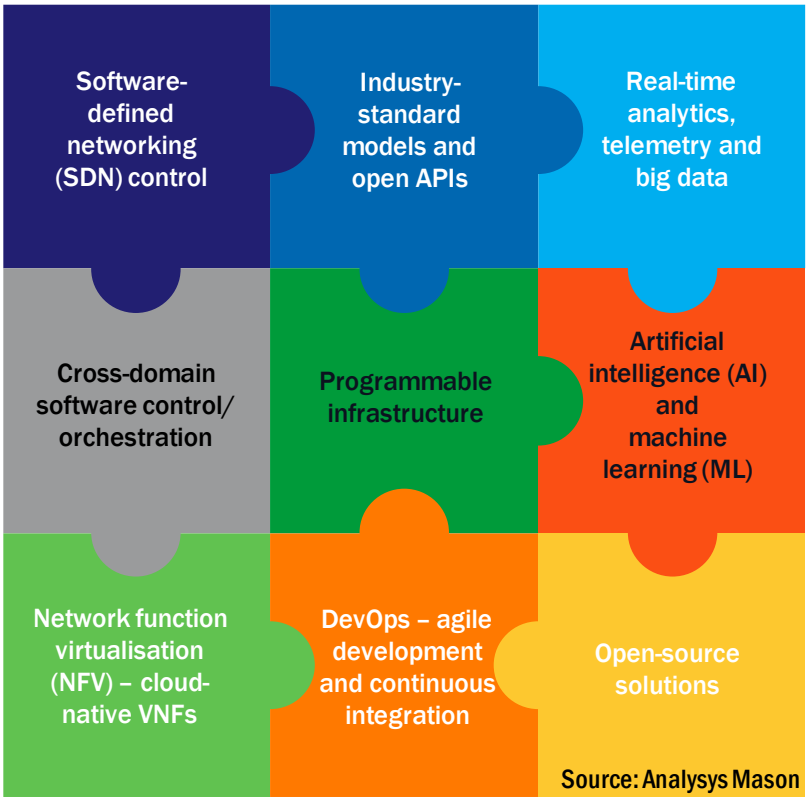
An adaptive network is a network that can self-configure, self-monitor, self-heal and self-optimize by constantly assessing network pressures and automatically reallocating resources, but is bound by the rules and policies set by the network provider and is under constant human supervision. These programmable networks will use continuous learning and optimization to dynamically adapt to changing service demands and traffic patterns; help network providers to reduce costs by enabling high levels of process automation and enhanced, AI- and machine learning (ML)-led and assisted decision making; and provide a high-quality customer experience with more predictive and proactive operations and differentiated SLAs.

AI-driven autonomous networking is a high-profile topic among network providers and their suppliers. AI/ML will be central to providers' efforts to create more-agile and leaner network operations, but that alone will not solve providers' critical networking challenges. An adaptive network embraces AI with human oversight and uses it in combination with a software-control layer and a programmable infrastructure (see section 3). These networks will put providers in control, rather than asking them to relinquish control to AI, by allowing providers to decide the strategic direction; set the constraints on the autonomous decision making with rules and policies based on business and operational objectives; and supervise autonomous processes and intervene as necessary. Overall, they will enable providers to complement human intelligence with artificial intelligence, where the strengths of one will compensate for the weaknesses of the other, and respond quickly and cost-effectively to customer demands and the competitive landscape.

Automating networks and their operations is not a new idea; providers have been pursuing the autonomous network vision for years. Many providers have adopted various tools and technologies to apply software-controlled, automated processes in various operational scenarios to certain degrees, such as for fault/alarm management, traffic management and RAN optimization, and more recently for Layer 1–3 service provisioning with software defined networking (SDN). However, these have typically been tactical solutions that have been implemented as disjointed, fragmented 'automation islands' for specific domains and services. Therefore, the overall level of automation in operations remains low, a long way from the desired goal of end-to-end automation and simplification across multiple networks and services.

Network providers are now presented with the opportunity to change this. The main building blocks of an adaptive network, such as SDN/NFV-based software control and automation, enhanced analytics-driven intelligence with AI and machine learning, and more-programmable network infrastructure (see Figure 1 and section 3 for detailed discussion of these components), are now available. They will enable providers to adopt a more strategic, embedded automation approach to make the network truly adaptive.

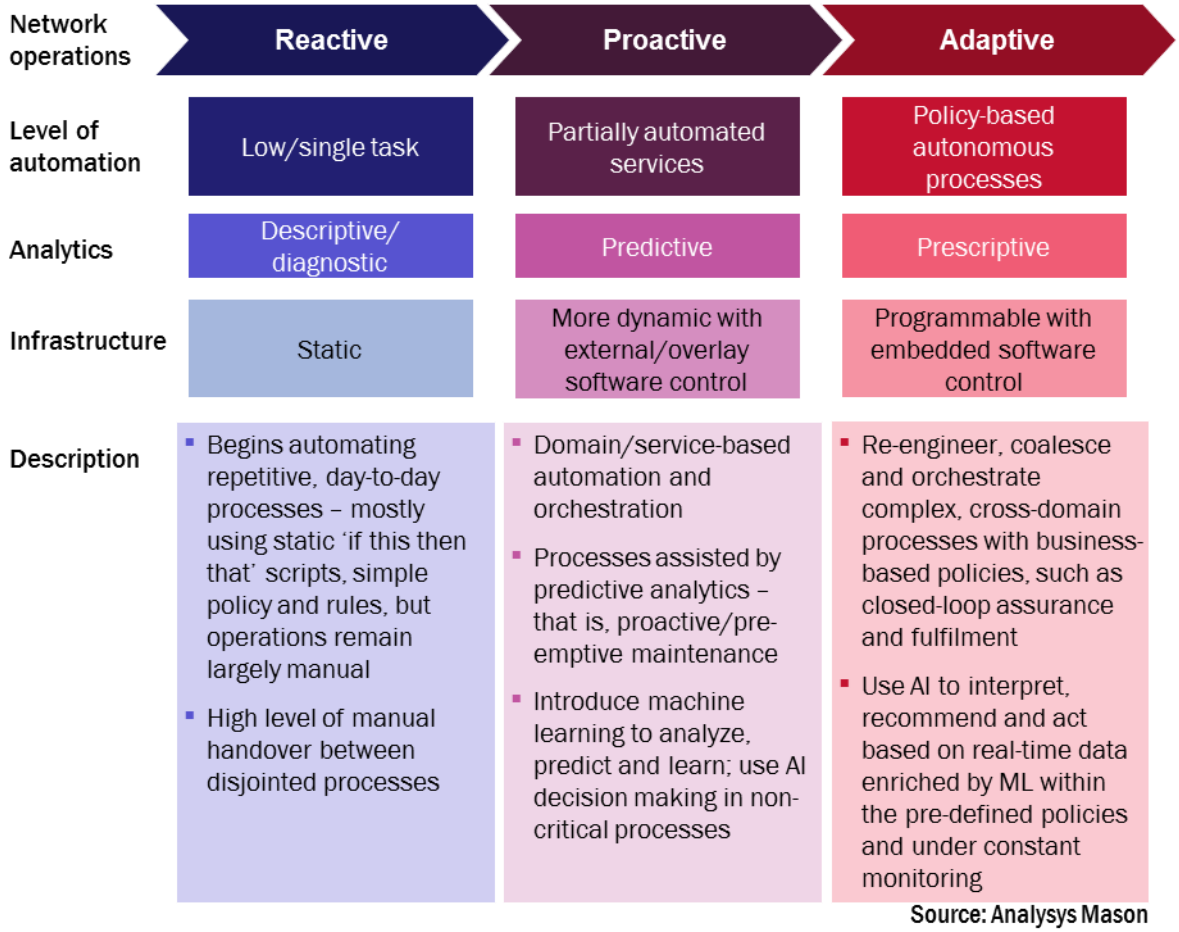
Figure 1: The building block technologies and tools of an adaptive network



The components of an adaptive network are at different stages of maturity and commercial adoption, but network providers should start now to create a long-term, end-to-end platform vision, join and meld these pieces together and plan for the operational and organizational change that will be required to fully realize the benefits. Leading providers have already begun to increase automation in specific network domains and services using SDN and NFV technologies (increasingly in combination, for example implementing SD-WAN and vCPE for enterprise service delivery); moving to DevOps-centric processes and open APIs; and applying advanced analytics and machine-learning techniques to smart infrastructure to improve network reliability by taking proactive actions.

Providers should take a step-by-step approach to building their adaptive networks (see Figure 2), with an end goal of bringing separate automated domains/services under end-to-end, cross-domain orchestration and closed-loop automated operations. Then providers can achieve AI-driven, more-intelligent and autonomous networks bound by their business policies and rules.

Figure 2: Evolution to adaptive network operations



2.2 Drivers and benefits of an adaptive network

Traditional wide-area communications networks are largely static, built with vendor-specific and special-purpose hardware network elements (NEs) and managed by multiple, distinct external operations support systems (OSSs) and element/network management systems (E/NMSs). This has led to complex, inflexible and disjointed networks and operations systems and vendor lock-in, and has hindered the improvement of automation and cost-efficiency in the design, integration, scaling and delivery of new services. Adaptive networks promise a significant opportunity for network providers to:

- **Improve network service agility to innovate faster and increase revenue** by transforming the highly fragmented and static nature of networks and operations towards adaptive approaches and improving long and opex-intensive service creation and provisioning cycles.
- **Control opex by increasing productivity**: a human-supervised and -programmed adaptive network can deliver the following productivity gains to providers:
  - protect/increase margins while scaling up networks and services without adding significant headcount
  - minimize human-error and reduce its associated operational risks
  - re-allocate skilled workforce from mundane, repetitive tasks to more-strategic and value-added activities directly aligned to business goals

- **Defer capex or redirect it to new growth opportunities.** Improved network and data center capacity allocation and increased utilization can allow providers to free up capex, which can be diverted to seek new market opportunities such as 5G, IoT/M2M, video etc.

The future mode of adaptive operations will be based on a highly automated and streamlined network service lifecycle. Providers' end goal with adaptive network operations should be fully integrated, policy-driven closed-loop automated operations across the service creation, fulfilment, assurance and network planning processes. This will require decomposition and migration of legacy software and process siloes to unified, end-to-end and centralized management and control of multi-vendor/multi-domain hybrid networks.

To decide where to better focus their investments, providers need a detailed understanding of the operations teams' tasks; where the time is being spent most and how automation can be applied to increase efficiency. Figure 3 identifies the main operational processes that can benefit from programmable infrastructure and an adaptive network.

Figure 3: Adaptive network future mode of operations (FMO) [Source: Analysys Mason, 2018]

Operations function	Adaptive network FMO
Service creation	• Faster and more cost-effective connectivity and communications service design, testing, integration, roll-out and continuous updates and improvements using DevOps principles
Order management and fulfilment	• Intent- and policy-based multi-layer service provisioning using model-driven service templates • Network self-configuration through software control to ensure intent and policy requirements are met • On-demand, self-service customer order, provision, monitor, change and terminate actions • Automated, remote delivery of services using SDN-based connectivity and VNFs, reducing on-site visits and simplifying design and deployment processes
Performance management and assurance	• Self-healing and proactive/predictive detection and resolution of network problems (failures, outages, performance degradations) before they occur, enabled by closed-loop automation between assurance and fulfilment systems, ML pattern identification and AI decision making • Reduced need for on-site visits due to such pre-emptive maintenance and remote problem resolution capabilities, along with enhanced self-service portals and automated care for rapid remedy • Rapid identification of, and protection against, malicious traffic with embedded security policies
Capacity planning and optimisation	• Self-optimisation, improved network utilization through closed-loop, policy-controlled automation with assurance/fulfilment systems and programmable infrastructure (e.g. variable bit-rate, software-configurable optics). An adaptive network can auto-scale in response to service demands, changing traffic patterns, policies and congestion by automated instantiation of virtual resources and SDN-based control of traffic flows, and configuration of programmable physical infrastructure • Reduced overprovisioning and worst-case design, and accelerated network planning processes thanks to continuous network and data centre capacity planning based on real-time data and advanced analytics and predictive planning and forecast capabilities

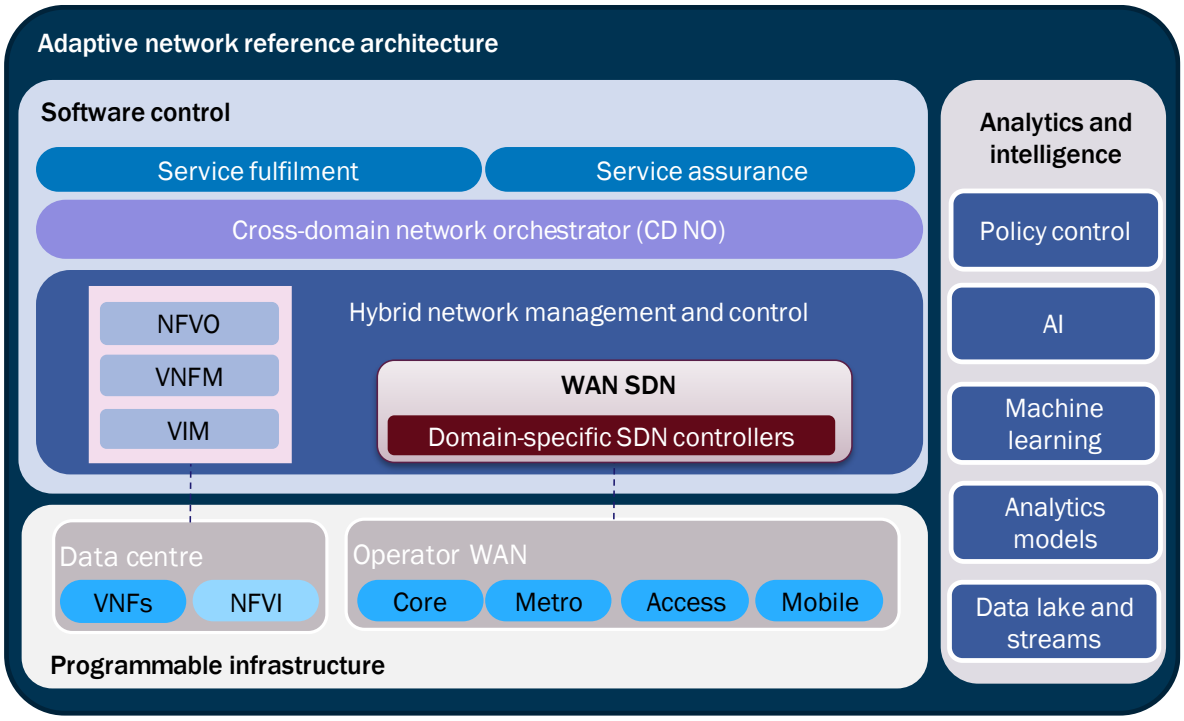
3. Key requirements for an adaptive network

3.1 Adaptive network reference architecture

Figure 4 illustrates how the various pieces of adaptive networks discussed in the previous section come together under three key architectural components, which are described in more detail in the following sections:

- **software control,** which forms the basis of adaptive operations by supporting the automated creation and deployment of network services at scale and speed using SDN, NFV and open APIs
- **programmable infrastructure,** a hybrid next-generation network that comprises open, SDN-enabled physical networks and cloud-native virtual network functions. A programmable infrastructure will provide advanced telemetry that delivers real-time data on the health of the network as well as the ability to tune to meet changing capacity needs.
- **analytics-driven intelligence,** which enables intelligent automation by enhancing autonomous decision making and supporting software-control through policy/rule engines, AI, machine learning and telemetry.

Figure 4: Adaptive network reference architecture



Source: Analysys Mason

Adaptive networks should be built based on the principles of openness, scalability, security choice and flexibility. Providers are looking for best-of-breed capabilities and want to be able to procure components/sub-components from a variety of suppliers, including open-source communities. To make these various hardware and software components work effectively with each other through open APIs, providers will need a coherent operational platform and integration framework that embraces all sub-components regardless of their source.[1] Security is also of paramount importance. Network providers must not only be able to secure their networks in

[1] Figure 4 provides a simplified view of what Analysys Mason calls a 'digital network and operations platform'. For more information, see www.analysysmason.com/defining-dnop-5g-rma16.

the face of rapid traffic growth, but also ensure the security of automated process so they deliver the business outcomes intended, and that only authorized users have access to key network management functions.

Software control for achieving intelligent automation and orchestration

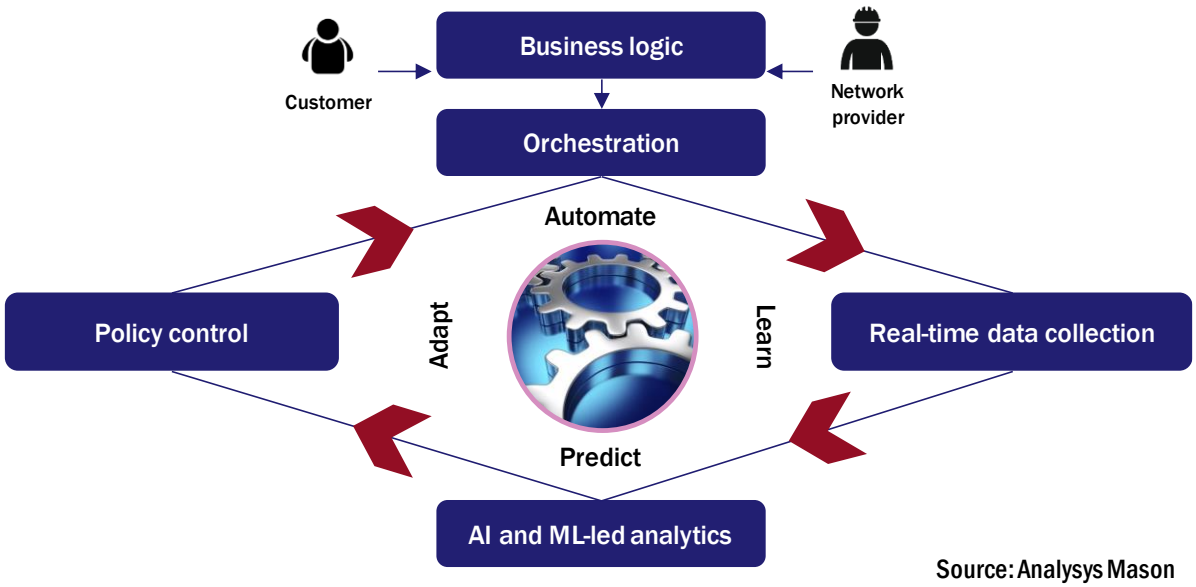
Software control in an adaptive network encompasses cross-domain network orchestration (CD-NO)[2], SDN control and NFV management and orchestration (NFV MANO). These functions collectively enable end-to-end automation in hybrid physical and virtual networks and across multiple domains (WAN, data center), layers (packet, optical) and vendor equipment and management and control software systems through open APIs.

Cross-domain orchestration acts as the brain of an adaptive network, supported by AI and policy

The CD-NO is an 'orchestrator of orchestrators'. It is the network's brain and is fundamental to the creation of intelligent networks that can support the level of service agility and adaptability to change. It collapses silos by abstracting the complexity of underlying network and IT domains and enables end-to-end, data-driven network service lifecycle orchestration and automation, working in conjunction with OSS (service fulfilment, service assurance) and customer-facing support systems.

Combined with analytics-driven intelligence and policy control (see section 3.1.2), CD-NO can help providers make the paradigm shift to the new mode of adaptive network operations that is based on automate, learn, predict and adapt cycles, as shown in Figure 5.

Figure 5: Software control network adaption cycle



Source: Analysys Mason

The CD-NO takes the role of an execution mechanism for closed-loop automated workflows and autonomous actions based on pre-defined policies and customer intent. It should manage and orchestrate WAN SDN controllers, E/NMS and NFV MANO and the programmable infrastructure through model-driven abstraction and open APIs/interfaces. For example, in provisioning an on-demand Layer 1 transport service, the CD-NO ingests and translates customer intent from a self-service portal and provides automated discovery and selection of ports using service templates. It then calls a path computation engine (PCE) to find the best route and stitch

2 Various CSPs and vendors also refer to CD-NO as a 'service orchestrator' (SO), "multi-domain service orchestrator' (MDSO) or 'network service orchestrator' (NSO).

the various domains together, and directs domain-specific SDN controllers to provision multi-vendor network equipment through open APIs.

WAN SDN control platforms are essential to implement network programmability

Application of SDN technologies (centralized network management and programmable flow control and device configuration) in adaptive WANs will be crucial to achieve dynamic delivery of network connectivity services and automation of manual provisioning tasks.[3] Providers have begun to deploy disparate tools to increase WAN automation: WAN configurators for automated, multi-vendor WAN device configuration; overlay SD-WAN solutions for traffic steering; and domain-/layer-specific SDN controllers to automate the management of individual networks. However, an adaptive network should be built using a platform approach that converges these various WAN SDN models into a single, open and modular WAN SDN control platform. Such a platform should provide:

- multi-layer, multi-vendor control by integrating domain-specific controllers and extending incumbent vendor and layer-specific E/NMSs and network control planes and domains without the need to disrupt or displace existing infrastructure
- centralized and converged management and control of multiple network layers that are traditionally managed separately (e.g. IP and optical)
- standard data modelling languages, protocols and APIs (i.e. TOSCA, YANG/NETCONF, MEF LSO, PCEP, and T-API) to enable providers to realize end-to-end, multi-vendor network lifecycle automation (planning, resource management, monitoring, assurance and provisioning). When integrated with the CD-NO and, as needed, the NFVO, WAN SDN platforms will allow providers to work with and around heavy and siloed OSS, and eventually phase them out.
- modularity to enable providers to pick and choose WAN SDN components/functionalities from various vendors and/or open source solutions.

3.1.1 Analytics-driven intelligence

To make their networks truly adaptive, providers should augment operational automation enabled by multi-domain orchestration with enhanced analytics and policy-controlled autonomous decision making. Providers will need advanced, embedded analytics capabilities in their networks that can aid self-learning from fast-changing environments; provide accurate predictions of potential network problems and anticipate trends; and ensure continuous improvement and adaptation of rules that govern autonomous operations. Figure 6 provides an illustrative analytics and intelligence architecture for closed-loop automated operations in an adaptive network. Figure 7 details its main functions and capabilities.

[3] Analysys Mason's WAN SDN definition encompasses SDN-controller driven and SDN-like deployments in CSPs' IP/optical access, metro and core WANs. For more details, see www.analysysmason.com/Research/Content/Reports/SDN-WAN-strategy-Mar2017-RMA07 and www.analysysmason.com/Research/Content/Reports/WAN-SDN-forecast-RMA07.

Figure 6: Analytics-driven intelligence architecture

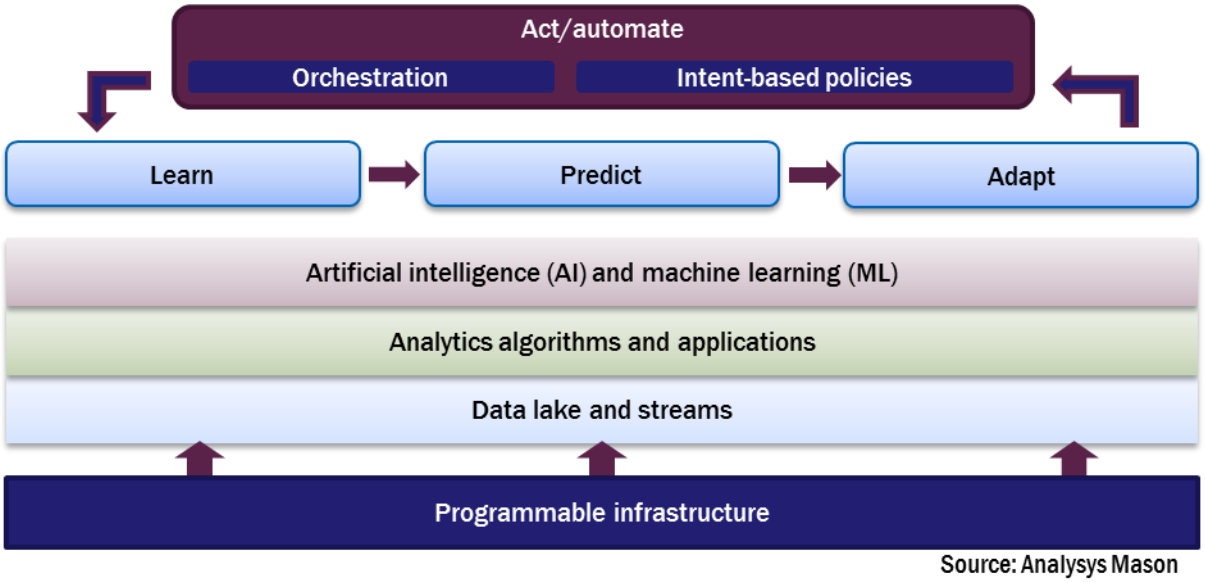


Figure 7: Analytics-driven intelligence functions and capabilities [Source: Analysys Mason, 2018]

Analytics and intelligence function	Capability description
Learn	• capture, store, analyse and correlate real-time and historical network and service data, including unstructured data • build algorithms and apply machine-learning techniques to identify patterns and extract new insight • support changing situations with unpredictable data sets and achieve self-learning
Predict	AI-assisted interpretation of datasets to: • detect anomalies to anticipate and avoid service disruptions and threats • support performance assurance and customer care • analyse traffic trends and capacity requirements to support proactive network planning • provide recommendations for optimal human decision making
Adapt	• dynamically update models, rules and policies based on positive and negative reinforcements for continuous improvement • ensure consistent change management through interworking with the software control layer

At the bottom layer of the architecture, there is a robust storage repository that will record, process and aggregate real-time and historical large-scale, raw data streams (such as log files and telemetry data) across the programmable infrastructure (in network and, as needed, the data center). This raw data should be processed, normalized and fed into the upper layers where advanced data models and analytics algorithms are used to generate actionable insights. AI and ML are general-purpose technologies; providers will need to apply a variety of machine-learning techniques based on the specific operational use cases and benefits they would like to achieve. For example:

- **supervised learning:** supervised machine-learning algorithms can be trained to identify patterns (e.g. degrading network performance), predict an outcome (e.g. port failure), trigger remediation actions (e.g.

auto-adjust network bandwidth, add new capacity). This type of ML is more commonly used and is suited for scenarios where historical data and outcomes are known

- **reinforced learning:** involves continuous calibration of the machine-learning algorithms based on feedback from its previous actions
- **unsupervised learning:** these algorithms use grouping or clusters to organize data to understand potential structures and enable the discovery of previously unknown/unnoticed patterns, i.e. identify new user/service traffic behavior/profiles to improve forecasting in network planning.

Policy control and AI/ML will collectively enable providers to design autonomous and adaptable troubleshooting, repair, configuration and mitigation processes. A policy platform incorporates the intent-based rules and conditions set by the provider and intelligently governs the behavior of an adaptive network. In a closed-loop automated process, the policy platform will evaluate the events, insights and recommended actions from AI/ML systems and will trigger the appropriate response through the software control layer. As the adaptive network continues to learn from its actions over time, these policies can be adjusted and updated to adapt the network to changes as dynamically as a provider's comfort level dictates.

3.1.2 Programmable infrastructure

An adaptive network will be based on hybrid, programmable infrastructure comprising physical and virtual network resources across the WAN and provider data centers that are managed and orchestrated by the software control layer.

Traditional provider WANs are highly stable and complex networks with multiple layers, protocols and services. In particular, optical transport networks are typically configured statically and engineered using worst-case, full-fill, end-of-life conditions. However, rapid and unpredictable growth in capacity requirements and competitive concerns require using network assets as fully as possible with minimal stranded capacity. Customer demands, too, push the need for more flexible, on-demand connectivity services enabled by more dynamic transport network architectures. Providers need infrastructure that can self-configure and self-optimize to meet the demands of existing services (cloud services, high-quality video, mission-critical enterprise services) and rapidly adapt to make way to future services (5G, network slicing, IoT/M2M).

Transport networks, due to performance and connectivity requirements, will remain largely physical rather than virtualized. Therefore, increased agility and configurability control will need to be achieved through implementing SDN, not NFV. However, simply adding external software control and intelligence to WAN infrastructure elements will not deliver the desired results if that underlying hardware is not adaptive as well and capable of supporting WAN automation. Example capabilities of an adaptive packet-optical network infrastructure that will enable WAN programmability include:

- variable bit-rate coherent optics that provide software-controlled, tuneable capacity across the transport networks (metro, core, data center interconnect and submarine) using real-time link data from the network, rather than worst-case estimates (see section 4)
- a flexible grid, reconfigurable photonic layer with colorless, directionless, and/or contentionless features that can dynamically reroute channels of variable spectral occupancy
- efficient, flexible mapping of client services to variable line capacity underpinned by a centralized or distributed optical transport network (OTN) or packet switching architecture.

The software to control these programmable network elements will not be locked away in single-vendor domains; it will be cloud-based and multi-vendor/multi-domain-capable, as described in the section on software control.

3.2 What should providers consider when building an adaptive network?

Figure 8 summarizes the common characteristics of solutions/components that providers should use to build their adaptive networks.

Figure 8: Adaptive network solution characteristics [Source: Analysys Mason, 2018]

Solution/component requirement	Description
Open and modular	Providers should be able to curate adaptive network components and functionalities from various vendors and open-source communities to achieve operational differentiation. These components should be supported by a large ecosystem and plugged into the appropriate software and hardware layers and enable automation and orchestration through open interfaces/APIs. Engaging with an integration partner can help providers bring these components together and ensure their interoperability.
Multi-domain/multi-layer support	This is a critical requirement for cross-domain orchestration and WAN SDN platform solutions. These solutions should provide providers with an end-to-end, unified view and autonomous control and management across physical and virtual network domains, layers and services, regardless of who supplies which network component.
Extensibility	Most providers will build their adaptive networks using a stepwise approach and thus it will be crucial to start with programmable infrastructure and WAN automation and analytics-based intelligence platforms that can support providers' development roadmaps and future services.
Standards-based	Adaptive network components should provide support for common, industry-standard APIs, protocols and data-modelling languages. This also includes compatibility with industry collaborations and standardisation groups.
Open development framework	The solutions or components should enable DevOps-based continuous development and integration by incorporating open-source components and exposing their capabilities.
Cloud-native architecture	Software solutions should be based on microservices-based architecture to best enable modularity, extensibility and scalability features.
Security	Network providers must be able to secure network traffic; guarantee the security of automated process so they deliver the intended business outcomes; and ensure that only authorized users have access to key network management functions.
Scalability	In an adaptive network environment, the network will need to scale dynamically to keep up with increases and decreases in demand on an as-needed basis.

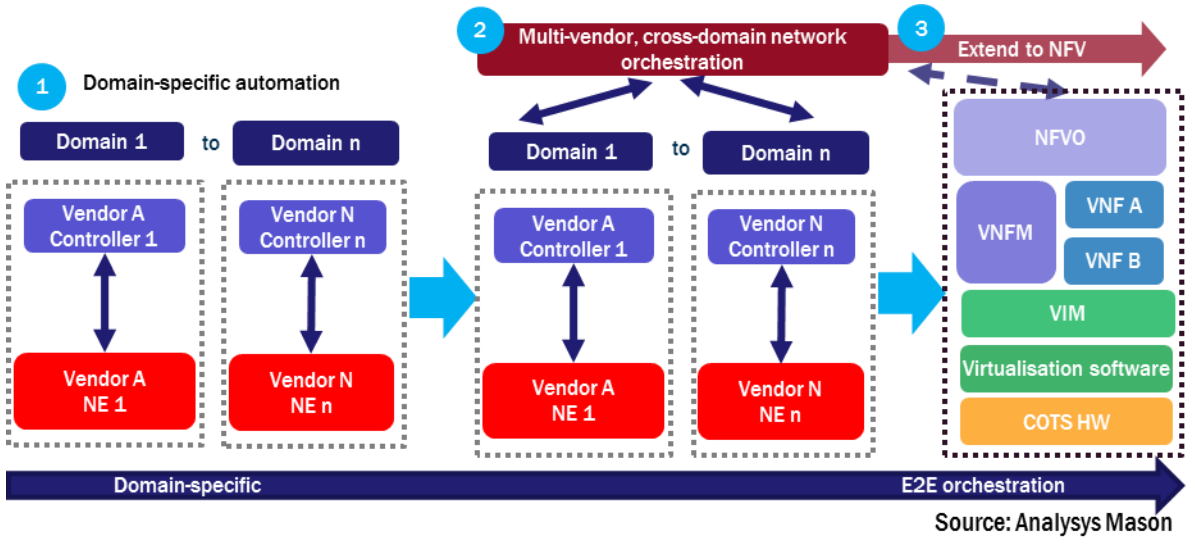
3.3 Migration paths for providers to adaptive networks

Each network provider will have a different path to the adaptive network, with unique starting points based on their existing network environment and business objectives. The more common approaches will be:

- A bottom-up, domain-specific automated control approach, applying SDN-based automation in individual domains/layers first, then moving to end-to-end orchestration over time and bringing SDN, NFV and programmable physical infrastructure together (see Figure 9).

- A top-down, end-to-end orchestration approach where providers start with the design and implementation of their coherent operational platform with CD-NO that will span their multiple network domains.
- A hardware-centric approach deploying programmable infrastructure coupled with analytics and open APIs to enable the network to become more adaptive and responsive to changing network pressures

Figure 9: Domain-specific orchestration approach, starting with specific domain(s)



A domain-specific, bottom up approach involves the following steps.

1. Implementing SDN-based automation in individual network domains, by replacing/extending E/NMS with SDN controllers typically provided by the incumbent network equipment vendor(s). Providers will follow different paths to individual domain automation, because they will prioritize the domains based on their business and operational objectives.
2. Coalescing these various SDN-controlled domains under a multi-vendor, multi-domain network orchestration layer (CD-NO), which will provide end-to-end connectivity control and management across the WAN.
3. Extending this architecture, as desired, by adding VNFs and data center/cloud resources to the CD-NO's remit.

Moving to end-to-end orchestration incrementally in domain-based steps can help providers minimize the operational disruption and target investment, therefore, most providers will prefer to adopt this approach. An example of this is Windstream's network automation project, as presented in detail in section 4.1.

Some providers will prefer to pursue the top-down approach, but the business case can be more difficult to justify and the complexity and disruption it involves can present a significant barrier. Analysys Mason estimates that less than 1% of all NFV/SDN deployments prior to 2018 have proceeded top down.

Still other providers will take an infrastructure-based approach that incorporates programmable hardware coupled with analytics and software tools to make their network more adaptable and provide a stepping stone to a bottom's up or top-down approaches.

Regardless of the path chosen, providers may need to seek external help from a professional services partner and trusted advisor; only a handful of providers have the required experience, skills and resources needed to

efficiently execute the architectural, operational and organizational shift to an adaptive network and manage its associated risks alone. Providers should choose partner(s) that can help them build their adaptive networks by integrating the software-based automation/autonomy control, analytics-based intelligence and the various programmable elements; provide DevOps, agile software lifecycle management skills; and support organizational/cultural change with proven industry expertise and best practices.

4. Adaptive network use cases

The following example use cases are among the more immediate opportunities for providers to explore as initial steps towards a more adaptive network.

- **Automated service provisioning with SDN:** providers can automate today's slow and costly manual service lifecycle processes in packet/optical networks by building an SDN-based multi-layer/multi-vendor automation platform and adopting DevOps processes. Section 4.1 provides a real case study of how a network provider (Windstream) automated the delivery of its wavelength services and plans to extend it to other services with a phased approach.
- **Proactive network assurance:** providers want to find and fix as many potential network problems as possible to increase network reliability and deliver differentiated SLAs and customer experience. A key step toward this end goal will be achieving pre-emptive network maintenance across the WAN (optical, Ethernet, and IP) by adopting network health prediction tools. Such tools, which are underpinned by AI/ML-enhanced analytics capabilities, can accurately indicate the likelihood of a network node's failure within a given timeframe for proactive repair.
- **Fiber capacity analysis and optimization:** policy-based matching of channel/wavelength capacity to available system margin enabled by programmable infrastructure and software tools can lead to more dynamic and efficient optical networks. Providers can optimize system margin utilization through better prediction of signal variability by combining real-time network telemetry data and improved traffic forecasting with AI/ML-led predictive analytics. By unlocking stranded capacity and its dynamic allocation, providers can improve network utilization and reduce cost-per-bit compared to traditional static design.

4.1 Windstream: Intelligent multi-layer/multi-domain network automation with SDN[4]

Business problem – operational complexity as a barrier against service agility

Windstream is a provider of voice, data and enterprise managed services in North America with an annual revenue of USD6.3 billion. It is operating in a highly competitive environment where operational efficiency and customer experience are crucial to meeting its market share and profitability goals. Because of its acquisition-based growth strategy, its network has become highly complex with many disparate systems and manual processes. This has resulted in long network service provisioning times and difficult and costly distributed device configuration updates. The provider needed a new network and service operations approach to increase

4 This is an excerpt of a case study that Analysys Mason wrote for Ciena with input from Windstream and Ciena. See www.analysysmason.com/contentassets/fdb0a40e2c1d43faa075bee86eab5028/analysys_mason_ciena_windstream_sdn_dec2017_rma16_rma07.pdf for the full case study.

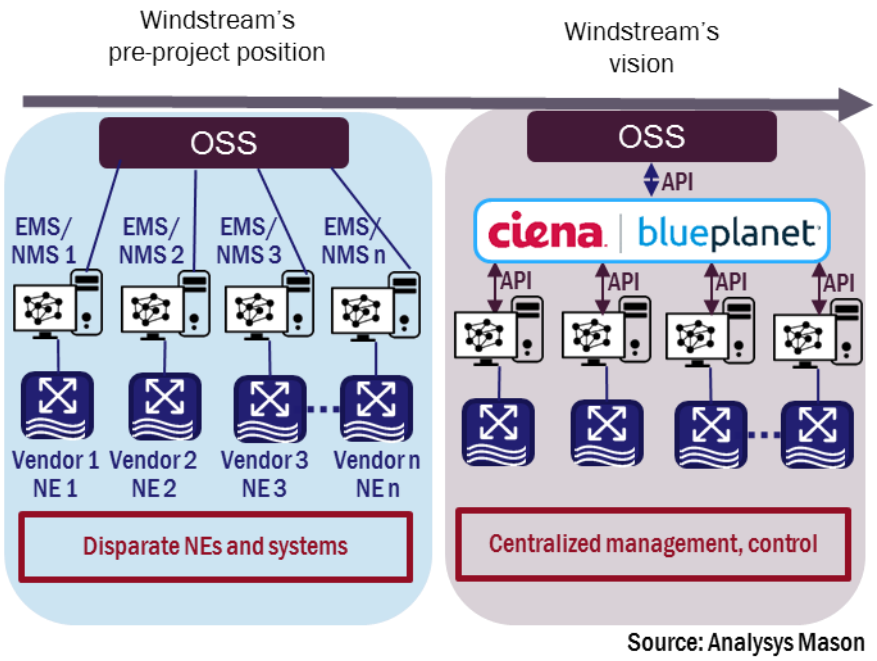
its service agility and automate the service lifecycle of its packet and optical infrastructure, which is the basis of its wholesale and enterprise services offerings.

Technical solution – a platform-based, phased approach to building an adaptive network

Windstream has embarked on an SDN-based network automation project to radically reform its B2B service processes and reshape customer experience. To achieve this, Windstream needed an open, extensible, model-based (e.g. TOSCA) network automation platform around which it could build new SDN-based automated services with a phased approach. As such, it has deployed Ciena's Blue Planet Intelligent Automation Platform to simplify operations and move to DevOps-centric processes.

The first stage of this project centered around the automation and orchestration of its optical network (including Ciena, Infinera, and Coriant optical infrastructure) to support wavelength services. Blue Planet-managed SDN allowed Windstream to launch its new Software Defined Network Orchestrated Waves (SDNow) wholesale 10G wavelength service with significantly reduced and predictable service cycles. Thanks to the platform's support for centralized inventory control and remote mass-configuration and software update of broad array of network devices from multiple vendors, the provider is now able to drastically simplify and reduce the cost of its operations. Figure 10 below provides a comparison of Windstream's network operations before and after the SDN project.

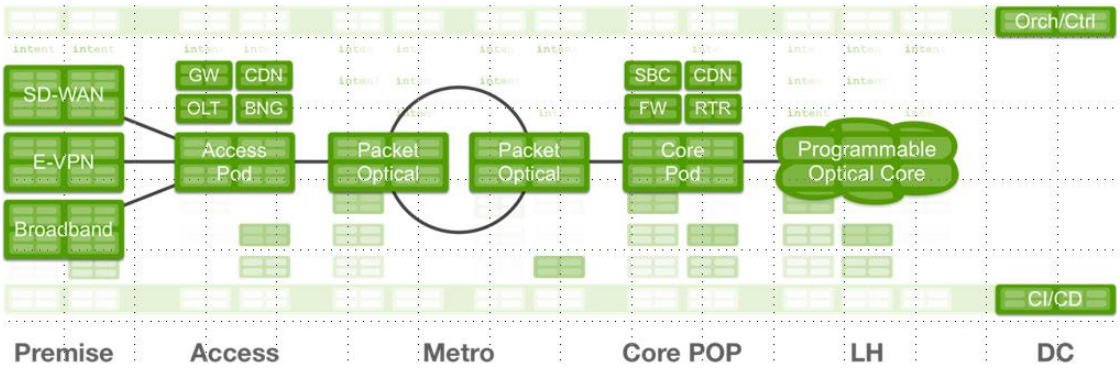
Figure 10: Comparison of Windstream's network operations before and after the SDN project



The provider, with support from Ciena, is also moving from a typical siloed, vendor/SI-delivered and planning-focused process based on a waterfall method to a collaborative DevOps-based, continuous development and release process focused on results. Using a DevOps approach to automate the foundation of its network will allow Windstream to add automation of Layer 2/3 equipment and adopt a continuous cycle of new product launches in the next 2 years.

Windstream is planning to add multi-layer/multi domain carrier Ethernet services for wholesale and enterprise services, and differentiated SD WAN offers incorporating universal CPE (uCPE) and service chaining. This will be followed by the incorporation of central office re-architected as a data center (CORD) or CORD-like infrastructure at the edge for software-defined access services. Windstream expects to compress cost and time to deploy consumer broadband network by 50% by extending its programmable network to the access edge. Figure 11 illustrates Windstream's end goal of building a highly programmable, automated and adaptive network.

Figure 11: Windstream's ultimate programmable network vision [Source: Windstream, 2018]



Windstream also wants to make its networks more accessible to customers through what it calls intent-based interactions: customers, on demand, will be able to make requests and not have to worry about the technical complexity behind their requests: the customer interactions will be translated into resources that need to be configured by the programmable network. To this end, the provider has collaborated on a PoC for intent-based, multi-vendor optical service orchestration of Layer 1 carrier services transporting ethernet with its vendor partners.

Benefits – a leap in service velocity and extensible platform for future services

Windstream achieved/expecting to achieve following benefits.

- **Improved operational agility and customer experience** thanks to much shorter and more predictable availability of 10G wavelength services. Windstream can for the first time guarantee 20-day service across its entire US footprint.
- **Improved cost efficiency** through centralized device configuration, software updates and inventory management, which should help reduce opex.
- **A platform for future service innovation.** Windstream has taken its first step towards its vision of a fully SDN-based network that decouples customer services from network devices. This will enable the provider to launch additional wholesale and business packet-optical services. It can also allow it to extend its programmable network to the access edge and create software-defined access services.
- **Fewer organizational barriers to success.** Art Nicols, Windstream's VP of Architecture and Technology, notes that "People and process are as important as systems – probably more so. Breaking down organizational barriers is long, hard work. Ciena has helped with this – getting the network and back office people together to talk through use cases, for example."

5. Conclusions and recommendations

Adaptive networks promise a revolutionary opportunity for providers to realize long-desired, highly automated, lean and agile operations. Providers should start now to build their adaptive networks and operations by joining the core components (programmable infrastructure, software control and analytics-driven intelligence) with a long-term, end-to-end platform vision that embraces the principles of best of breed, openness, scalability, and security. However, this doesn't have to be a large-scale transformation project with major disruptions. Providers can improve network automation, programmability and adaptability by using a stepwise, phased approach, as discussed in section 3.3, and breaking its implementation down to smaller, incremental steps to minimize the operational disruption and risks, and achieve the benefits along the journey.

Moving to adaptive network operations will involve significant technological, operational and organizational/cultural change, and providers will be faced with many challenges. The following recommendations and best practices can help providers overcome perceived barriers and get on the path to building an adaptive network.

- **Establish priority and timing** for what parts of the network to make adaptive based on clear business strategies and goals. Network and network operations are complex. 'Rip and replace' is costly and disruptive, but a plan based purely on end-of-life replacements is likely to take too long and result in persistent islands of adaptability. A strategic whole WAN plan – worked through with the help of an able, trusted partner, as required – will help guide investment and quicken returns.

- **Bring the pieces together:** The plan should include a vision of how all the pieces of an adaptive network will come together. Adaptive network ingredients will likely continue to mature at different rates. Providers may need help integrating the pieces together and keeping them updated, but they should have a long-range vision that guides their construction of adaptive networks.

- **Start staff retraining/reorganization and process reengineering very early on:** Some processes will need to be re-designed specifically for automation and adaptive networking. Jobs will change from performing direct action on the network to programming effective policies and supervising decisions made by an adaptive network. For example, providers can re-allocate some of their operational staff, whose tasks are being automated, to newly-established policy management teams which will be responsible for the creation, testing, validation, monitoring and continuous adaptation and improvement of adaptive network policies. Expertise as well as trust will build over time. Focus on reengineering/retraining and reorganizing staff and processes in concert with the business priorities to maximize return.

- **Control the risks of autonomy:** providers are naturally averse to ceding the running of their networks to algorithms. First, poor automation/automated decision-making in workflows could have significant adverse impact on the network and services. Second, any network outage could have serious negative consequences to a provider's reputation and finances. Providers will need to grow confidence in adaptive networking over time. Controlled adaptation (i.e. autonomous processes may seek approval from operations staff for the mission critical decisions before they act, or they can be designed 'fail-safe'- no decisions can be taken autonomously if they cannot be undone) can help increase providers' comfort level. Again, partnerships with system integrators or other trusted solution providers can help assess and mitigate concerns and remove risks. Increasing decision-making autonomy step by step as noted in section 3.1.1 (from supervised learning to reinforced learning to unsupervised learning, for example, or starting with conservative, fixed policy control then implementing dynamic, machine-learning based policies) is another way to grow

comfortable with autonomous adaptability. Implementing autonomy with a minimal disruption strategy is also wise.

- **Select the right partners to support your journey:** The evolution of the adaptive network is a long journey with many challenges along the way and providers may benefit from engaging with external partners who can bring the expertise and professional services to effectively execute the architectural, operational and organizational shifts that an adaptive network will require.

Investments in adaptive WANs will pay off for providers in more streamlined operations; faster network innovation; more agile enterprise and wholesale service and data center interconnections; and better utilization of network assets while containing opex and deferring capex or redirecting more of it to growth opportunities. These benefits collectively provide a significant competitive advantage to truly adaptive providers. Investments can and should be paced to support a provider's financial and other business goals, and should not require massive 'rip and replace' or 'transformation' projects.

About the authors

Gorkem Yigit (Senior Analyst) is the lead analyst for the Service Delivery Platforms programme and a contributor to the Software-Controlled Networking and Network Orchestration programmes, focusing on producing market share, forecast and research collateral. He started his career in the telecoms industry with a graduate role at a leading telecoms operator, before joining Analysys Mason in late 2013. He has published research on NFV/SDN services business cases, identity management in the digital economy, and has been a key part of major consulting projects including Telco Cloud Index and IPTV/OTT procurement. He holds a cum laude MSc degree in Economics and Management of Innovation and Technology from Bocconi University (Milan, Italy).

Dana Cooperson (Research Director) is the research director for Analysys Mason's network-focused Software Research programmes. Her area of expertise is intelligent fixed and mobile network infrastructure. Her goal is to help customers strengthen their link in the communications value chain while evolving their business operations to benefit from, rather than be threatened by, shifts in the market. The key network infrastructure trends Dana focuses on include the integration of communications and IT assets and the drive towards software-controlled, virtual networking.

This white paper was commissioned by Ciena. Analysys Mason does not endorse any of the vendor’s products or services.

Analysys Mason's consulting and research are uniquely positioned

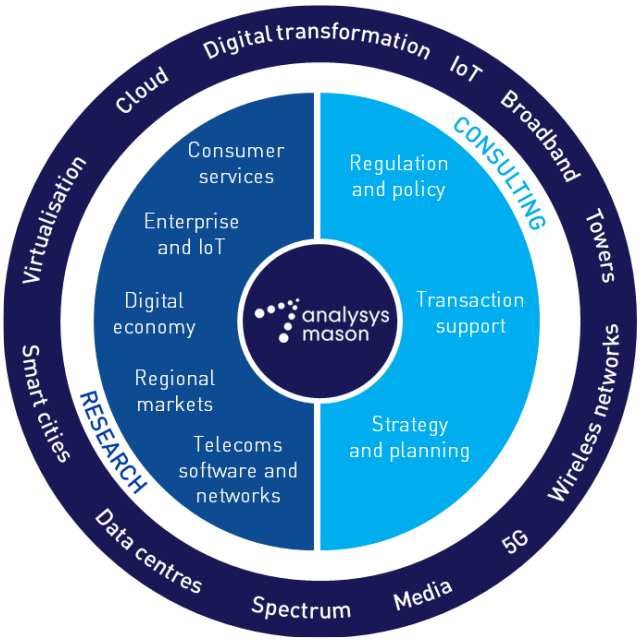
Analysys Mason is a trusted adviser on telecoms, technology and media. We work with our clients, including communications service providers (CSPs), regulators and end users to:

- 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 more than 220 staff in 13 offices and are respected worldwide for exceptional quality of work, independence and flexibility in responding to client needs. For 30 years, we have been helping clients in more than 100 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

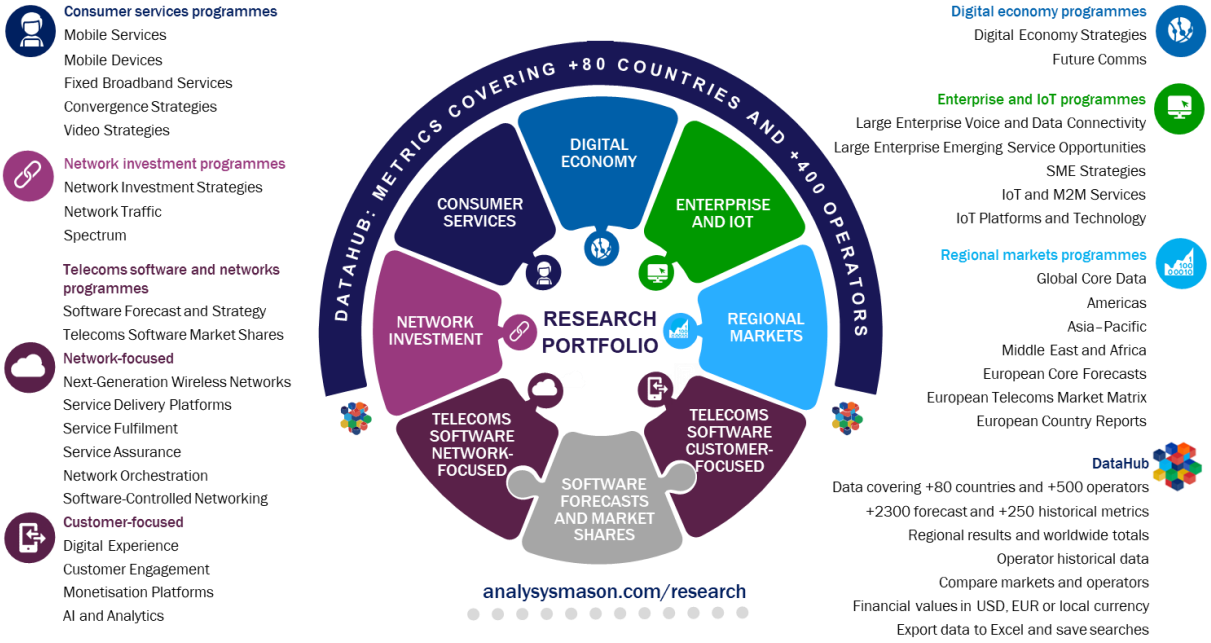
- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

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.



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

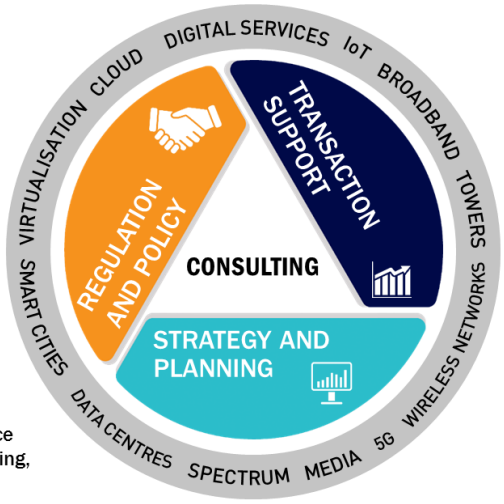
For 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities

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

- Quality of service
- Market review
- Margin squeeze tests
- Analysing regulatory accounts
- Regulatory economic costing
- Policy development and response
- Media regulation
- Expert legal support
- Radio spectrum management
- Net cost of universal service
- Radio spectrum auction support
- Postal sector policy: universal service obligation (USO), liberalisation, costing, pricing and regulation



TRANSACTION SUPPORT

- Commercial due diligence
- Technical due diligence
- Mergers and acquisitions (M&As)
- Debt and initial public offerings (IPOs)
- Joint-venture (JV) 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.