analysys mason

Perspective

Building operator NaaS platforms: the crucial role of cloud-native, disaggregated IP networks

July 2022

Gorkem Yigit

Contents

List of figures

This perspective was commissioned by DriveNets. Usage is subject to the terms and conditions in our copyright notice. Analysys Mason does not endorse any of the vendor's products or services.

1. Executive summary

1.1 Disruption is due in the enterprise connectivity market

A combination of workplace trends, digital transformation, Industry 4.0 supply chain transformations and edge is driving enterprises' demand for connectivity that flows between any endpoint and cloud and adapts itself to applications and security postures in a completely programmable way. However, the current fragmented approaches and technologies for enterprise networking are failing to provide the frictionless, on-demand cloud experience that enterprises are looking for. Traditional operators, in particular, are struggling to deliver this cloud connectivity and the related value-added services in a timely and cost-efficient manner, and are faced with stagnating legacy service revenue and increasing capex and opex associated with their legacy network infrastructure.

Traditional operators that want to meet the new market demands and maintain their relevance will need a digital platform from which they can provide connectivity and related value-added services on demand. Advanced traditional operators have recognized that such a digital platform is the foundation for what they are calling 'network-as-a-service' (NaaS). Operators' underlay networks (WAN transport, core, interconnect, aggregation and edge) will remain critical to NaaS platforms in order to meet SLA and quality-of-service (QoS) guarantees, especially for mission-critical applications, and to allow enterprises to consume network resources using an on-demand, as-a-service model. However, operators need to architect and build their underlay networks differently in order to deliver NaaS.

1.2 Traditional operators must embrace IP network clouds to build their NaaS platforms

Building the underlay network as an end-to-end IP network cloud is a key component of a NaaS-driven, WAN/IP network transformation. IP network clouds represent a return to the original principles of software-defined networking (SDN) in the WAN; this is, to provide a centralized, programmable control plane that is separated from the user plane. This control plane allows the instantiation of any network service on the correct user plane infrastructure in order to meet enterprises' bespoke connectivity requirements (such as those related to geography, QoS and cloud access). The separation of the control plane from the underlying physical networks in an IP network cloud allows NaaS operators to simplify the user plane and optimize costs and performance by using open, disaggregated hardware technologies such as merchant-silicon-based white boxes and cloud servers.

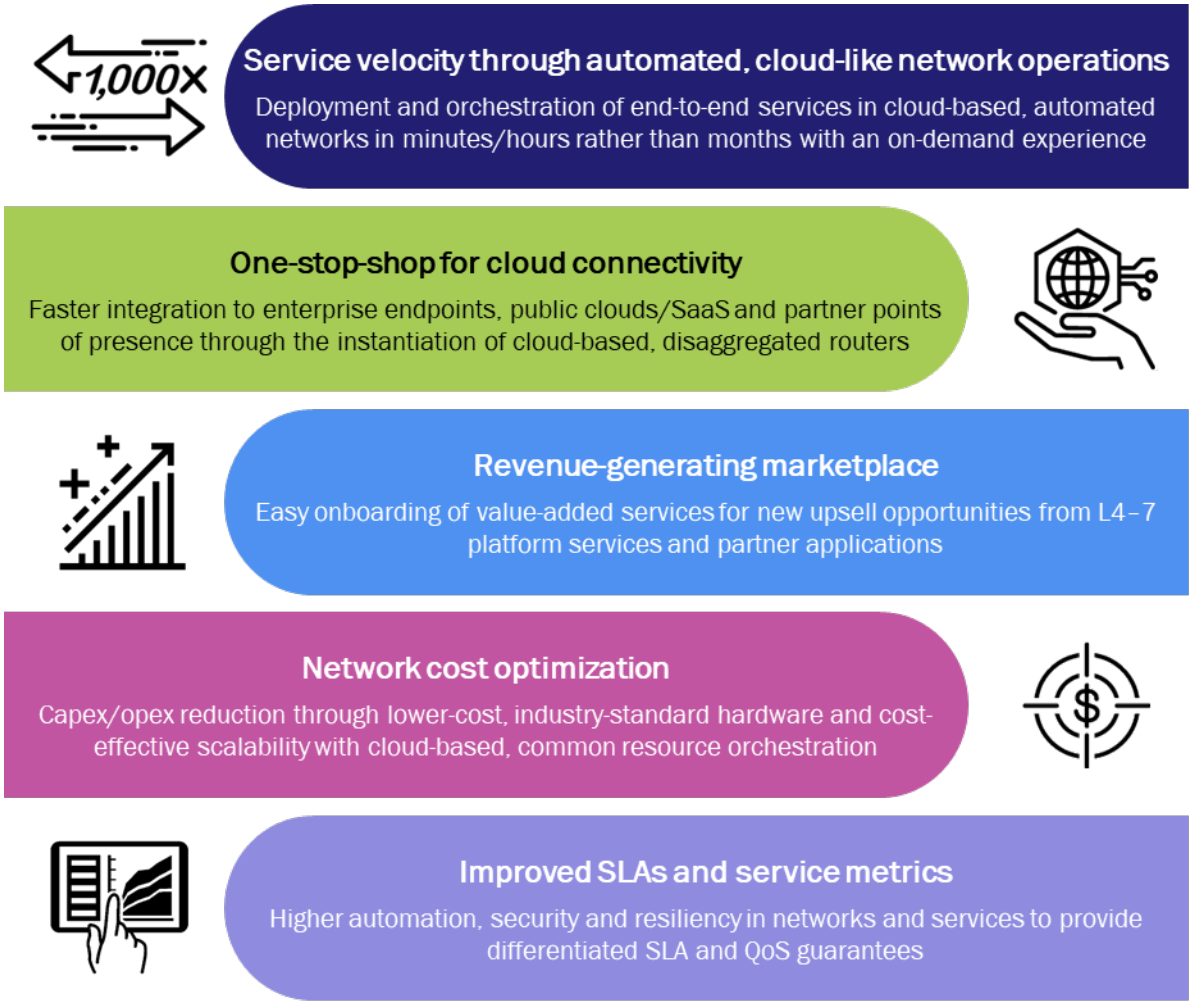
An IP network cloud also opens up the possibility of co-locating value-added L4–7 microservices in the same cloud environment as the centralized control plane. This means that NaaS operators can reduce the service chaining challenges associated with discrete L4–7 appliances (which can take at least 6 months to set up) by providing single pass processing. This enables operators, together with third-party partners and developers, to build orchestrated NaaS marketplaces that appeal to enterprise customers that want to reduce their vendor and technology complexities.

© Analysys Mason Limited 2022

1.3 IP-network-cloud-based NaaS platforms will set a new benchmark for service velocity, innovation and cost economics and could reset the enterprise connectivity landscape

IP network clouds are highly disruptive but offer the greatest pay-off for NaaS transformations. Improved service velocity, innovation, market differentiation and cost optimization are the main benefits because IP network cloud architecture involves radical network simplification to address cloud connectivity challenges and alter network cost economics with a streamlined, open hardware infrastructure (Figure 1.1). In addition, operators that implement an IP network cloud will be highly cloud-native and software-capable, and will benefit from zero-touch automation across Day 0, 1 and 2+ processes. These operators will be able to create and deliver services much more quickly and cost-efficiently than traditional service providers and will generate revenue at their expense.

Figure 1.1: Main benefits of a NaaS platform underpinned by an IP network cloud



Source: Analysys Mason

1.4 Building an IP network cloud will require a long-term vision and the right set of partners

This paper lays out the key requirements and building blocks for creating a successful NaaS platform based on an IP network cloud. Traditional operators that are planning to achieve this end goal will need:

© Analysys Mason Limited 2022

- common, unified IP network cloud architecture across multiple network domains, which includes a cloud-native control plane and an orchestration platform with strong hardware abstraction capabilities
- a modern operational model for an IP network cloud and NaaS that is based on automated lifecycles of open, disaggregated hardware and software components
- suitable technology partners who can provide expertise and end-to-end operational support
- open platform APIs and developer tools to cultivate a rich ecosystem of partners
- a software-capable organization with cloud, automation and disaggregated networking skillsets.

2. Key market trends in the enterprise cloud connectivity market

Enterprises' accelerated digital transformation in the post-pandemic era is driving the overhaul of IT architecture into decomposed, containerized cloud-native microservices that are hosted in public (IaaS, PaaS and SaaS) and hybrid cloud-based environments. Many enterprises are adopting a combination of multiple public cloud services (AWS, Azure and GCP) in conjunction with Salesforce, Office 365 and cloud-based unified communications-as-a-service (UCaaS), as well as secure access service edge (SASE)/zero-trust network access (ZTNA) services for remote workers. In addition, enterprises are preparing for emerging Industry 4.0 operational technologies (OT) as well as greater supply chain diversification and localization, which is increasing the demand for highly distributed, time-sensitive and secure clouds. Analysys Mason's research shows that 87% of large enterprises will increase their budget for cloud computing and secure remote access in the next 12 months,[1] and 80% of enterprises expect to purchase edge computing services in the next 5 years.[2]

All of these trends are spurring a rapid change in enterprises' networking requirements and the connectivity market landscape. Technologies such as SD-WAN, and its offshoot SASE, do not entirely address enterprises' network connectivity needs. SD-WAN that relies on best-effort internet is not always an ideal solution for many enterprises due to the potential reliability and security issues for mission-critical applications and sensitive data in transit. SLA-based underlay network connectivity with QoS guarantees to transport data to and from clouds remains essential. Enterprises are increasingly in need of a single network that combines the programmability and deployment flexibility of SD-WAN/SASE with the advantages of the underlay IP transport network.

Traditional operators are repositioning their connectivity offerings and related service portfolios for the cloud connectivity market, but they are struggling to implement the required level of flexibility and service velocity. Operators' legacy IP transport networks, which are based on vendor-proprietary, pre-integrated routing platforms, are not built for end-to-end programmability, and operators have to rely on a limited set of vendors to add new service features. These factors are bringing cost and delay into service provisioning, thereby resulting in a loss of business to more-nimble competitors.

1 For more information, see Analysys Mason's Large enterprise telecoms usage and requirements: business survey 2022.

2 For more information, see Analysys Mason's Large enterprises' demand for communications and IT services: survey results 2021.

© Analysys Mason Limited 2022

2.1 Enterprises demand a simple, consistent way of provisioning connectivity and related L4–7 services between multiple clouds and application locations

In the new era of cloud connectivity, enterprises need to connect a multitude of clouds, applications and end users to each other in a timely and agile manner. They also need to deploy and manage L4–7 services (such as firewalls, SD-WAN, WAN optimization and other security services) over this highly distributed networking fabric. However, enterprises are facing significant challenges in achieving these goals due to the following factors.

- **Fragmented connectivity services landscape.** Enterprises and their service providers need to stitch together a complex set of networks and services across a disparate connectivity landscape. Traditional operators are building direct connections to public clouds, but these typically lack programmability and do not extend to the long tail of SASE, storage, content delivery network (CDN) and data center providers. Public cloud providers (PCPs) are building networks (such as AWS Direct Connect and Azure ExpressRoute) that only connect their own locations and are providing their own native networking and automation constructs, which cannot be easily replicated elsewhere. A growing number of software-defined cloud interconnect (SDCI) middle-mile network providers are emerging in the market to fill the gaps, but they usually have limited geographical footprints. Overall, it is a highly manual, inflexible and costly process for enterprises to patch together connectivity to clouds and data centers over these fragmented networks.

- **Siloed network technologies and operations.** Each underlay network and overlay technology provider brings different sets of capabilities, proprietary tools and interfaces, which leads to siloed operations and complex maintenance and support activities. This also makes it difficult to apply traffic engineering, telemetry and security policies consistently across different networks and gain end-to-end network visibility.

- **Complex service chaining.** Many enterprises need to manage multiple L4–7 services that consist of discrete, traditional appliances or NFV-based functions from a variety of vendors such as Checkpoint, Cisco, Fortinet and Palo Alto. This adds to the multi-cloud connectivity challenge because these functions are not yet cloud-native and may be deployed on-premises or as SASE services from specific clouds. This means that they require service chaining, which is currently complex and time-consuming to set up.

- **Lack of cloud-native development support.** CloudOps and DevOps teams in large enterprises are increasingly becoming the buyers of network services. They wish to configure and provision network infrastructure as a code as part of their CI/CD pipelines using common tools such as Terraform or Ansible.

All of these connectivity requirements and challenges highlight the market need for network-as-a-service (NaaS) solutions that provide a single, automated self-service interface for enterprise and cloud networking services, with on-demand service provisioning and flexible consumption models. Traditional operators that want to offer successful NaaS propositions must find a new way of building and operating their IP transport networks if they want to differentiate themselves in this highly competitive market and counter the threat from alternative service providers.

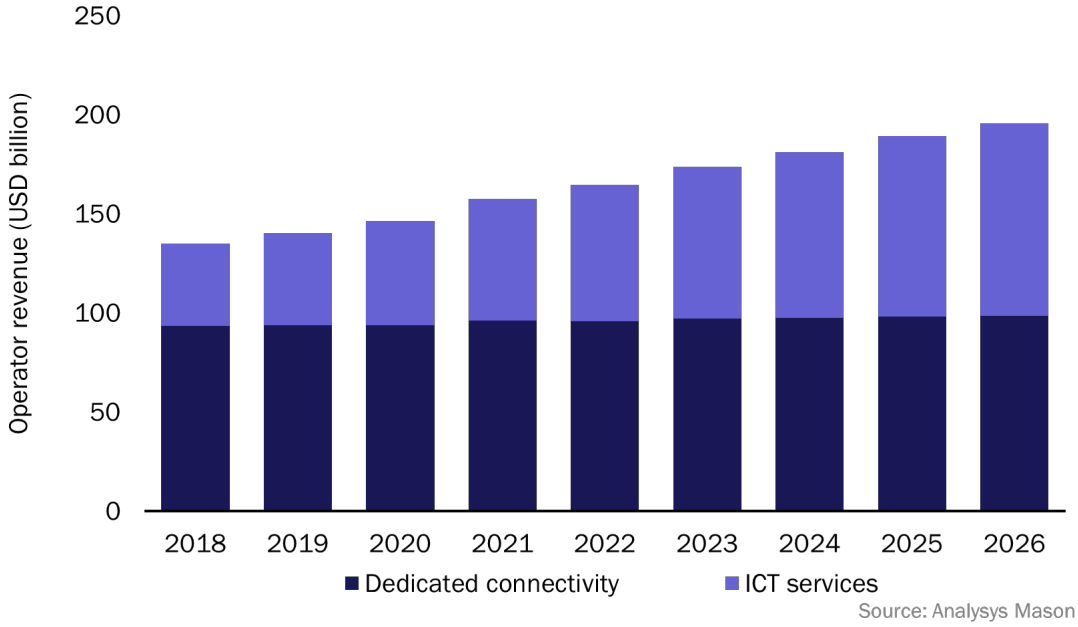
Section 3 of this report analyses the emerging NaaS landscape and traditional operators' challenges related to developing NaaS platforms while using legacy networks. Section 4 provides an overview of the ideal NaaS platform architecture for operators and the key building blocks and features to realize this architecture.

© Analysys Mason Limited 2022

3. Operator challenges and threats in the new era of distributed, multi-cloud networking

Traditional operators are currently the key suppliers of connectivity and value-added information and communications technology (ICT) services (cloud, security and enterprise mobility) to enterprises of all sizes. Dedicated connectivity services (MPLS, Ethernet, digital leased lines and ATM) represent operators' largest revenue stream from enterprises, but this revenue has been stagnating or declining. Indeed, dedicated connectivity services revenue grew at a CAGR of just 0.7% worldwide between 2018 and 2021 (Figure 3.1). New value-added services have compensated for the loss in traditional connectivity revenue.

Figure 3.1: Total operator revenue from enterprise connectivity and ICT services, worldwide, 2018–2026



Operators are increasingly offering managed SD-WAN services and often partner with multiple SD-WAN vendors such as Fortinet, Versa and VMware to bundle these services with their IP transport networks in order to capitalize on the growing demand for multi-cloud and branch connectivity. However, the trend is shifting toward relying more on SD-WAN and overlay services and reducing the spend on, and importance of, more-lucrative MPLS services, even though many enterprises use traditional MPLS and SD-WAN in a hybrid mode. As such, traditional operators are looking for new approaches to make their IP networks more agile and programmable so that they can enhance and differentiate their connectivity offerings and avoid conceding revenue to new entrants/challengers.

Cloud-based, value-added ICT services for enterprises will deliver strong long-term revenue growth prospects for traditional operators, as shown in Figure 3.1. Indeed, the results from Analysys Mason's survey show that 30–40% of large enterprises are considering buying additional ICT services (security, SaaS, co-location and unified communications) from their main connectivity provider.[3] This indicates a big upsell opportunity for

[3] For more information, see Analysys Mason's Large enterprises' demand for communications and IT services: survey results 2021.

operators who build a broad portfolio of services that are delivered over a highly flexible and resilient underlying IP transport network that spans a wide range of clouds and geographies. However, the cost (capex/opex) and time associated with the creation and delivery of these rich connectivity and value-added services will be critical in determining the competitiveness of traditional operators. Operators are generally struggling to meet the increasingly complex and demanding needs of cloud networking in an agile and cost-efficient way. This is mainly a result of their legacy, vendor/domain-specific and service-specific network appliance and operational silos, which lead to the following challenges.

- **Slow lead times and an inability to provide an on-demand service experience.** Network infrastructure complexity across legacy, disparate and closed vendor technologies prevents operators from consistently applying SDN and automation to agile service creation, provisioning and monitoring processes and exposing these processes to empower end users with self-service capabilities.

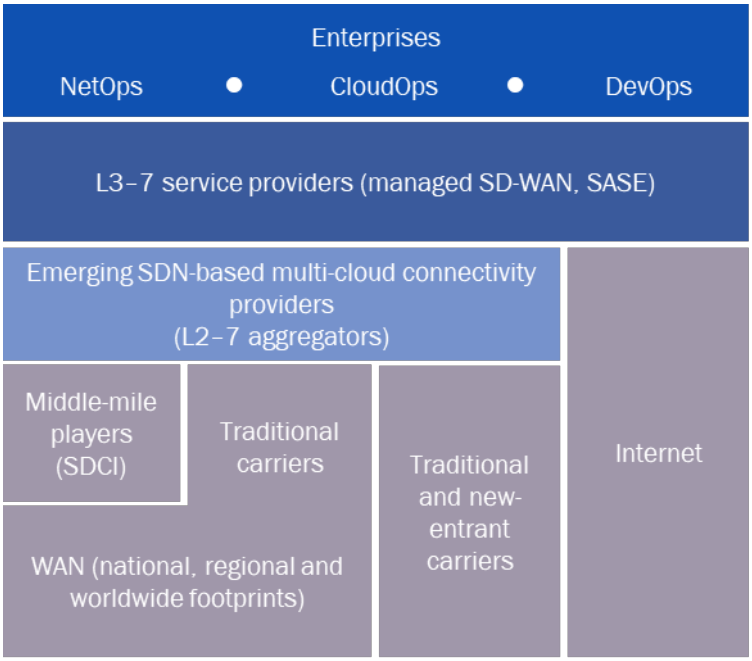
- **Opex-intensive, manual operations.** Network and service lifecycle processes over legacy operational silos are highly manual and lead to large headcounts and slow, costly and error-prone operations. This poses significant risks in meeting SLAs and key service metrics (such as the mean time to repair and uptime) for advanced cloud networking services.

- **Limited and expensive innovation.** Creating and deploying new connectivity services is vendor-dependent and often requires slow, expensive roll-outs of new hardware appliances. This leads to high capex and opex bills when operators want to diversify their service portfolios, and limits their ability to offer new, flexible pricing/commercial models.

3.1 Traditional operators are facing strong competition from modern, alternative service providers in the enterprise connectivity market

The market trends and challenges discussed so far mean that there is a growing risk of traditional operators being disintermediated by alternative service providers (or even enterprises that are building their own networks). Changing enterprise requirements in the distributed, multi-cloud networking era are reshaping the competitive landscape and driving the entry of new, nimble players, such as Alkira, Cato Networks, Packet Fabric, Teridion and F5/Volterra, that are filling the gaps in the enterprise cloud connectivity market (Figure 3.2). PCPs (including AWS with Cloud WAN and SiteLink and Azure with Virtual WAN) and co-location providers (such as Equinix and Digital Realty) are also making substantial investments in their WAN connectivity services. These services enable enterprises to connect to public clouds directly through points of presence, which may negate the role of traditional operators' networks. As such, traditional operators risk being bypassed and/or replaced by the other players in the enterprise connectivity value chain if they do not move fast enough to transform their networks and service capabilities.

Figure 3.2: Enterprise cloud connectivity market landscape



Source: Analysys Mason

3.2 Traditional operators need to shift to NaaS with new cloud-based IP transport networks to counter the threat

Enterprises are increasing the number of cloud services that they use, but they want to streamline and simplify their relationships with suppliers of connectivity and related network services by buying more services from fewer providers. Indeed, the results of an Analysys Mason survey show that 80% of enterprises want to reduce their number of connectivity suppliers.[4] This indicates that there is a strong market opportunity for service providers that can build a digital NaaS platform with a large service partner ecosystem that provides a one-stop-shop for most enterprise connectivity needs.

The NaaS market is still nascent and is in a land-grab state. There are significant opportunities for traditional operators who can transform and establish themselves as NaaS platform providers with a strong market presence in a timely manner. Operators are in a good position to capitalize on this opportunity because they have more experience in delivering SLA-based services than emerging competitors. They also have existing enterprise relationships and large network/connectivity assets. However, operators face a huge amount of competition from many different players, as discussed in Section 3.1. Operators' IP transport networks will be foundational to their NaaS connectivity services, and operators need to differentiate and futureproof these networks with new, radical architecture that is based on cloud technologies and principles. Such architecture will allow them to:

- gain programmable and flexible control over routing in their IP transport networks
- enable the rapid and cost-effective development of connectivity and related services across different domains and layers

4 For more information, see Analysys Mason's Large enterprises' demand for communications and IT services: survey results 2021.

- achieve more-sustainable and powerful zero-touch, intent-driven automation based on cloud-native tools and skillsets.

4. Unified, cloud-native and disaggregated networks provide the foundation of operators' NaaS platforms

4.1 Overview of an ideal NaaS platform and key architectural features

Traditional operators are increasingly recognizing the need to develop NaaS propositions that cater for enterprises' evolving networking requirements and desire to consolidate their connectivity suppliers to reduce service complexity. Several advanced operators, such as AT&T, BT, Colt, Lumen, PCCW Global and Verizon, are spearheading the industry's NaaS ambitions. They are building digital NaaS platforms that provide a unified, intent-based network experience that is underpinned by open, programmable IP transport networks. Figure 4.1 gives an overview of an ideal NaaS platform and Figure 4.2 outlines the main platform characteristics and features.

Figure 4.1: Overview of a digital NaaS platform

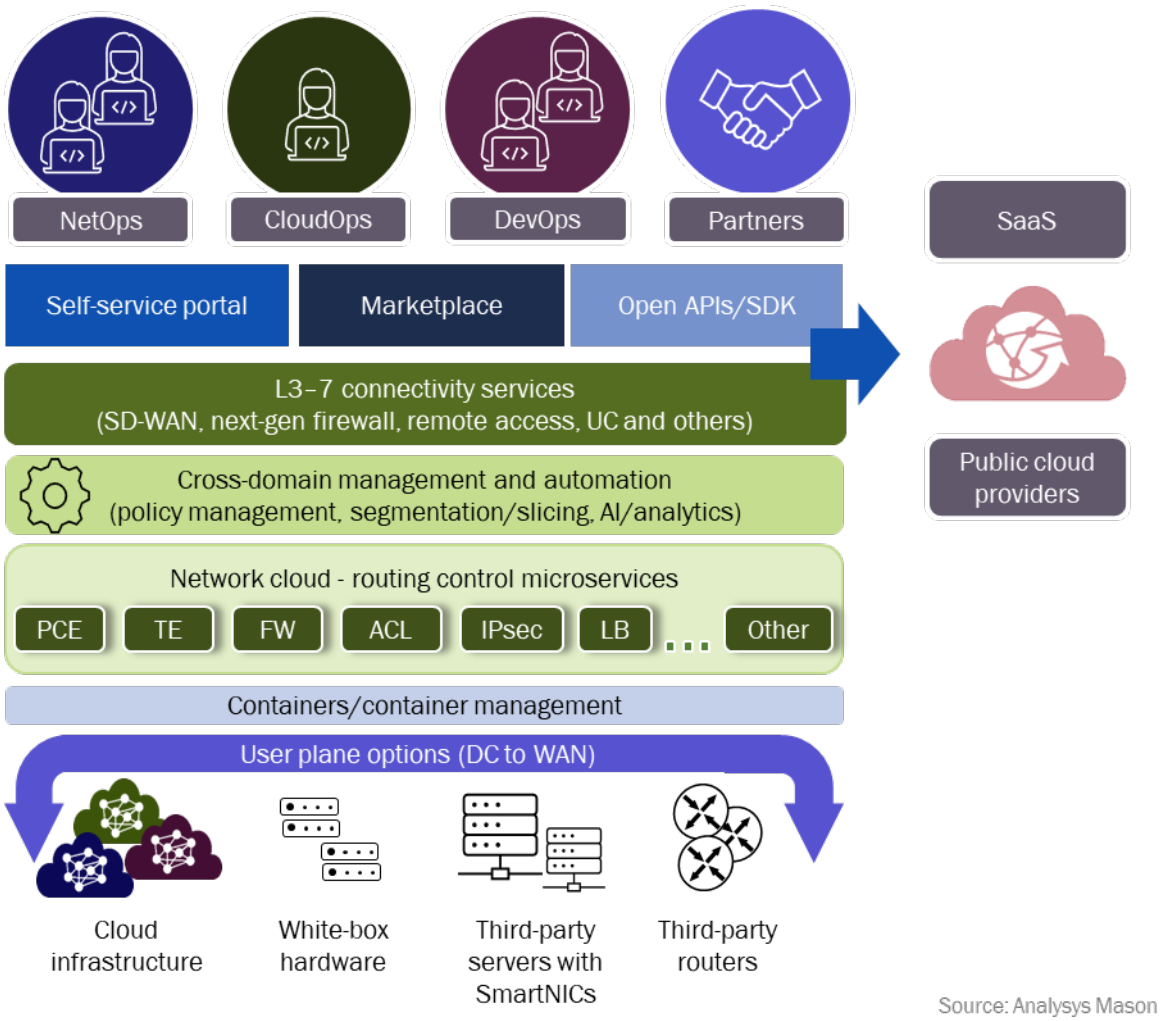


Figure 4.2: Main characteristics and features of operators' digital NaaS platforms

Characteristic/feature	Definition
Multi-underlay connectivity and orchestration	• Integrates the currently dispersed and fragmented network domains and extends into partner infrastructure (such as that from PCPs, other operators and SDCI/middle mile providers) • Network-agnostic orchestration enables connectivity from anywhere to any application in any cloud and provides multiple global transport and access options (enabled by MEF APIs or 5G APIs for network slicing)
L3–7 services marketplace	Offers a broad portfolio of third-party partner and operator self-developed value-added services such as SD-WAN, security, remote access, cloud and unified communications services through an open marketplace
Self-service portal	• UI-based self-service portal provides on-demand, automated provisioning, configuration and up-and-down scaling of connectivity and network services • Provides single-pane-of-glass management and visibility of all services consumed from the platform
Flexible commercial/pricing models	Ability to offer all services with cloud-like consumption-based pricing (per user, bandwidth or use case) and an opex model
API exposure	Exposes platform capabilities through open APIs and SDKs for third-party developers and DevOps and CloudOps teams

Source: Analysys Mason

4.2 A cloud-native, disaggregated IP network cloud is essential for NaaS platforms

As discussed in Section 3, existing, legacy network infrastructure hinders operators' ability to develop advanced enterprise cloud networking services such as NaaS and automated network operations. To build a complete, competitive NaaS platform as described in Figure 4.1 and Figure 4.2, operators need to rethink and transform their underlying network and service architecture, from last-mile access to WANs (metro, edge and core) and data centers, using cloud-native, SDN and automation technologies.

Operators have been on a long journey to transform their networks with cloud and automation technologies. Cloud-based software functions are already pervading mobile networks from the mobile core to the edge and RAN. However, the way in which operators build and operate their WAN underlays (IP core, metro, aggregation and access) has not changed significantly over many years. Operators will need to alter their IP network paradigms as they look to develop new NaaS models and platforms. They should design and operate their IP networks like clouds, with hardware-decoupled, software functions and platforms in a similar way to hyperscalers and cloud providers.

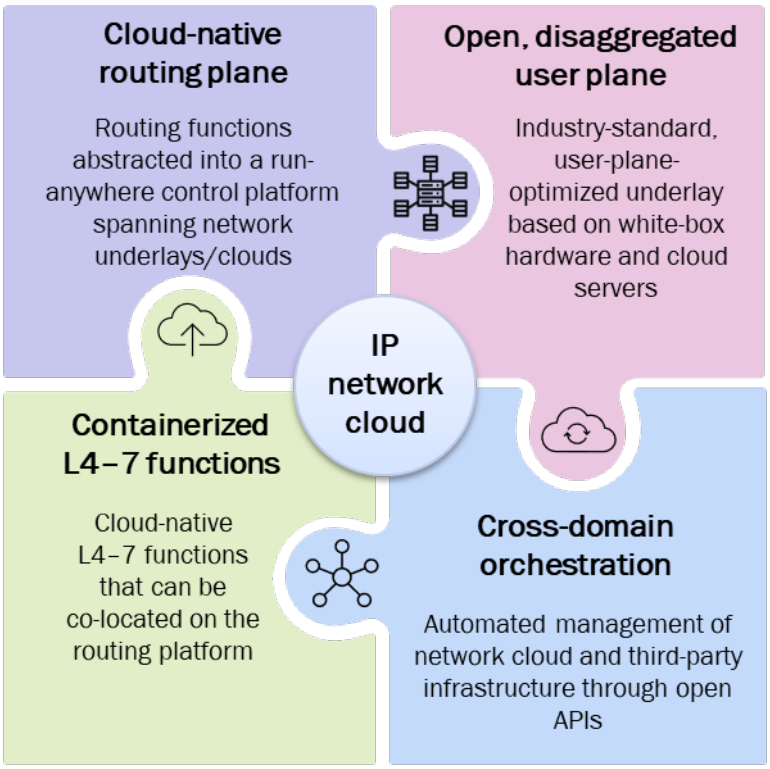
An end-to-end IP network cloud that collapses domain- and service-specific silos and converges network routing and L4–7 applications into a single cloud-native platform is a key component of a NaaS-driven, WAN/IP network transformation. A unified, cloud-native routing plane that spans multiple network domains with an open ecosystem of L4–7 functions and common management could replace the complex network and service environments that enterprises and service providers have today. Figure 4.3 illustrates the key technology building blocks and architectural principles of an IP network cloud that includes:

- **a cloud-native control plane** based on control and user plane separation (CUPS), where the routing functions and logic are extracted out of physical routers and deployed as software-defined, containerized

control plane microservices in a network cloud that can be spun and run anywhere, including private and hybrid/public cloud environments

- **an open, disaggregated and user-plane-optimized underlay** that consists of industry-standards-based white-box/merchant-silicon hardware clusters and cloud servers that are highly performant and programmable and support the deployment of any function and service in the network cloud
- **cloud-native L4–7 functions** that can be co-located with microservices-based control plane instances in the network cloud so that enterprise traffic can be micro-segmented and processed in a single pass to address the current service chaining challenges
- **cross-domain network and service orchestration** for the automated management of the cloud-native routing plane, disaggregated underlay and third-party infrastructure and traditional routers through open APIs.

Figure 4.3: Key pillars of an IP network cloud for a NaaS-driven transformation



4.3 Network disaggregation enables the convergence of routing plane and overlay services for the delivery of end-to-end connectivity services

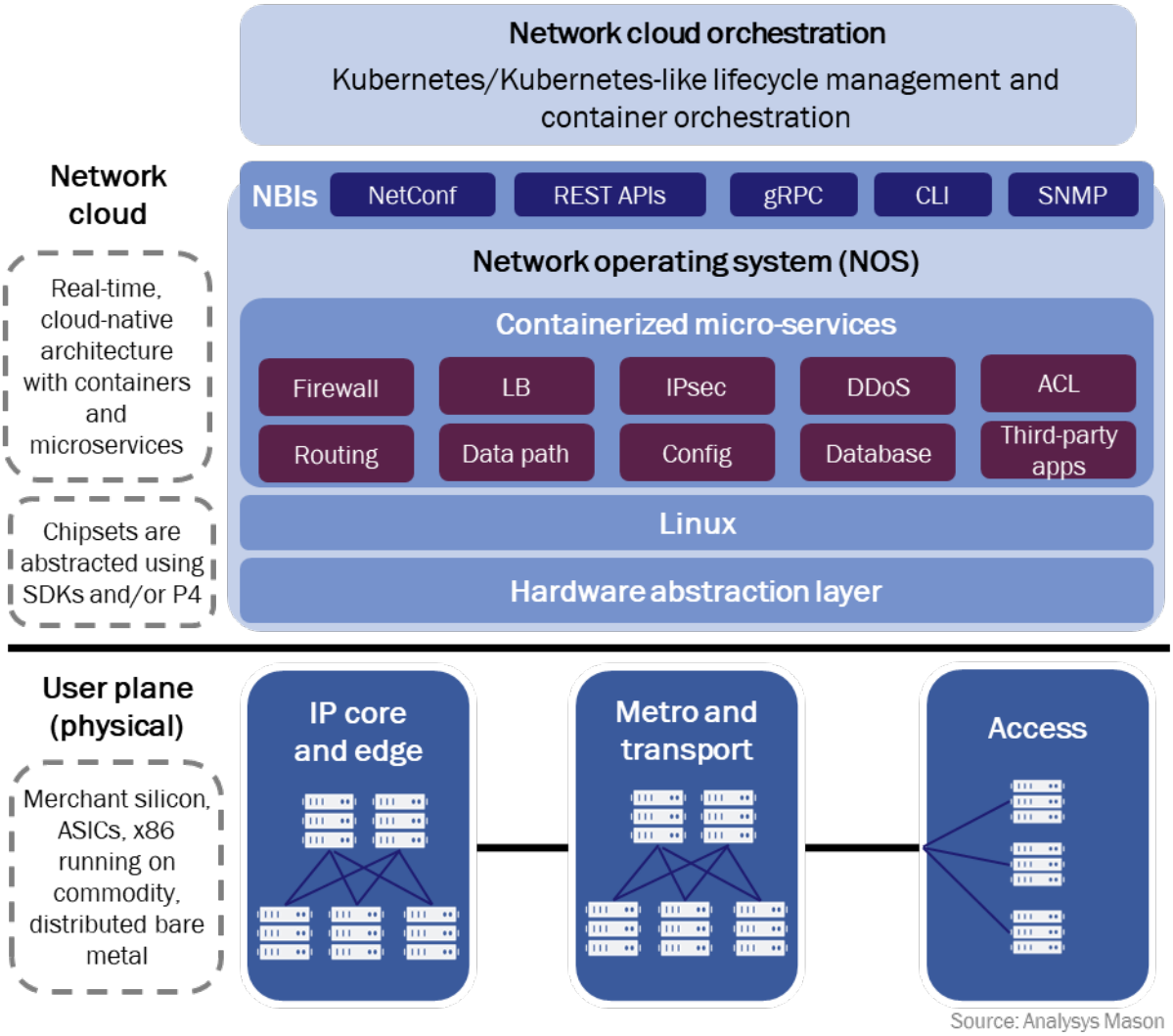
Disaggregated networking is at the core of hyperscalers' and cloud providers' network strategies. It enables them to mix and match open software and hardware components to gain cost advantages and increase service innovation, supply chain control and automation. Operators are increasingly exploring whether network disaggregation strategies and benefits can be achieved in their own network transformation initiatives. Indeed, there is a growing momentum of applying various disaggregation approaches in operator WAN transport, aggregation and access networks. AT&T and KDDI are prime examples of operators whose disaggregated IP core and edge networks use distributed disaggregated chassis (DDC)/disaggregated distributed backbone routing (DDBR) architecture. An increasing number of operators are also implementing disaggregated cell site routers,

cloud broadband network gateways (BNGs) and optical line terminals (OLTs).[5] Industry initiatives such as Telecom Infra Project (TIP) and Open Compute Project (OCP), which are supported by a fast-growing ecosystem of technology suppliers and operators, are putting significant efforts into developing disaggregated networking standards and facilitating their adoption.

Network disaggregation lays the foundation for a more open, granular and cloud-based network environment, as illustrated in Figure 4.4. The decoupling of network hardware and software enables the separation of the network control/routing and user/data planes. This allows the **control plane functions** to be rearchitected as cloud-native microservices, and enables their deployment in an IP network cloud platform. The IP network cloud also abstracts the **underlying open, data plane infrastructure**, which can be simplified and standardized using highly performant and cost-optimized white-box hardware based on merchant silicon (such as that from Broadcom) and cloud servers in a scale-out topology. As a result, operators can build a centralized control/routing plane for the deployment and management of any network service across their various underlying infrastructure domains. This enables operators to instantiate and allocate network services on the correct user plane infrastructure in order to meet specific cloud connectivity requirements (such as those related to geography, QoS and access options) and scale out network capacity cost-efficiently by simply adding new white boxes.

5 For more information, see Analysys Mason's Telco network disaggregation tracker.

Figure 4.4: Overview of IP network cloud architecture



Several advanced operators are already working toward building their IP network clouds, starting from specific domains and services. These clouds can evolve into an end-to-end platform as operators expand into the rest of their networks and look to host other workloads and network functions such as L4–7 services and third-party applications. Leading L4–7 application vendors have started to re-engineer their appliance- and/or VM-based functions to be cloud-native microservices. **Co-locating the L4–7 functions** with the **cloud-native routing control plane** can enable customer traffic to be processed in a single pass and therefore reduce the service chaining complexities of discrete, multi-vendor appliances. This creates the opportunity for operators to build an orchestrated marketplace that consists of a broad portfolio of value-added services that can help them to differentiate and further monetize their NaaS platforms.

A cross-domain orchestration platform is a key component of an IP network cloud and is responsible for achieving zero-touch automation in NaaS lifecycle operations and disaggregated underlay infrastructure management. The orchestration platform should work together with the cloud-native routing control plane to provide automated service templates that are agnostic to the underlying infrastructure's specific capabilities. These templates can be parameterised at run time(that is, when they are deployed or orchestrated) in order to instantiate services on the correct user plane infrastructure to meet an enterprise customer's business intent and requirements for cloud access, QoS and geographic redundancy. The orchestration platform should continuously

self-monitor and optimize services after they have been provisioned to maintain intent and SLAs with minimal overhead.

4.4 Key benefits of building the transport networks of a NaaS platform based on an IP network cloud

Cloud-native, disaggregated IP network clouds will lead to the convergence of network-, cloud- and application-layer technologies on a unified, multi-service platform that removes the fragmented networks and operational silos caused by dedicated appliances for specific functions and features. The key advantage of this architecture is that abstracting the underlying complexity of underlay networks, overlay networks and services will allow operators to expand their NaaS proposition quickly by enabling:

- faster integration to enterprise endpoints, PCPs and middle-mile network points of presence through the instantiation of software-based, disaggregated routers on any cloud to address multi-cloud connectivity
- the rapid ingestion and configuration of new underlay networks and partner infrastructure through APIs (such as MEF APIs) to expand connectivity options and footprint
- the deployment and orchestration of end-to-end services in a cloud-based, automated environment in minutes rather than months
- the enrichment of underlay connectivity with more-advanced and performant traffic engineering and advanced routing capabilities (such as segment routing) to make the underlay networks more valuable than just transiting traffic
- higher flexibility and resiliency in networks and services than is available from competitors with rigid architecture and slow operations.

5. Conclusions and recommendations

It is becoming essential for traditional operators to transform their existing network infrastructure and operations as enterprise customers look to reduce their network complexity and deploy more connectivity use cases. Operators should provide modern NaaS offerings that meet the needs of enterprise and cloud connectivity with an on-demand service experience and SLA/QoS guarantees. A cloud-native, open and multi-service IP network cloud platform should be at the core of these NaaS-driven transformations to enable the radical network simplification and cloud-based automation that is needed to set a new benchmark for service velocity and network cost economics. The IP network cloud is a major paradigm shift from existing approaches to IP networking and requires a long-term vision and plan. We provide the following recommendations to operators that are considering building modern NaaS platforms that are underpinned by an IP network cloud.

- **Operators should plan for a common, unified IP network cloud architecture across multiple network domains.** Operators can start building their IP network cloud from singular domains based on their immediate business and operational objectives, but they should have a long-term, end-to-end platform vision as they expand into the other parts of their networks. Operators should use a common, open architecture and reusable platform components that will enable them to adapt and replicate the initial deployments horizontally across the network and provide a unified, cloud-native control plane and orchestration environment with strong hardware abstraction capabilities. Operators will also need to extend the orchestration and management of existing infrastructure elements because these will co-exist in a hybrid

© Analysys Mason Limited 2022

network environment. This will require an IP network cloud platform to support common interfaces (Netconf, OpenConfig and gRPC) for northbound and southbound integrations.

- **Operators should adopt a modern operational model for the IP network cloud and NaaS that is based on automation and economies of scale.** The lifecycle of hardware and software in an IP network cloud involves a series of activities (solution design/validation/integration, supply chain management/logistics, Day 0,1,2+ processes and support and upgrades) that are handled by a mixture of operators, integrators and vendors, so operators are not familiar with all of them. Operators will need to invest in process automation and must change their network planning and design activities to ensure the viability of disaggregation and to maximize the benefits. Operators should consider working with vendors and professional services partners or industry bodies (such as TIP) who can provide built-in automation and zero-touch automation capabilities and assume the responsibilities and risks of the IP network cloud lifecycle and vendor ecosystem more-efficiently with large operational scale.

- **Operators should ensure the openness of their IP network cloud to support a rich ecosystem of partners.** Unlike the traditional monolithic router model, the IP network cloud model facilitates partnerships, which are an essential part of NaaS offerings to address many enterprises' preferences for particular clouds/technologies/vendors. Operators need to make sure that their IP network clouds provide open APIs and developer tools/SDKs that expose infrastructure capabilities to enable easy integration with partner infrastructure (such as that from PCPs, other operators and middle-mile partners). They must also enable the development and deployment of third-party microservices to build a broad portfolio of value-added services.

- **Operators should invest in organizational change and training/upskilling to achieve software-mastery.** NaaS and IP network clouds represent a major deviation from the current way in which operators build and operate their networks. Operators need to become more software- and automation-capable by having the right sets of IT, cloud and disaggregated networking skills to play in an increasingly software-defined enterprise connectivity market and regain control of their networks. Their ability to grow their NaaS businesses will depend critically on having skilled network engineers and operations teams that can build and deliver new services and features in the control plane, orchestration platform and self-service portals.

© Analysys Mason Limited 2022

6. About the author

Gorkem Yigit (Principal Analyst) is the lead analyst for the Cloud Infrastructure Strategies research programme. His research focuses on the building blocks, architecture and adoption of the cloud-native, disaggregated and programmable digital infrastructure and networks that underpin the delivery of 5G, media and edge computing services. He also works with clients on a range of consulting projects such as market and competitive analysis, business case development and marketing support through thought leadership collateral. He holds a cum laude MSc degree in economics and management of innovation and technology from Bocconi University (Milan, Italy).

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.

We reserve the rights to all intellectual property in this publication. This publication, or any part of it, may not be reproduced, redistributed or republished without our prior written consent, nor may any reference be made to Analysys Mason in a regulatory statement or prospectus on the basis of this publication without our prior written consent.

© Analysys Mason Limited and/or its group companies 2022.