What is NaaS and why is it important?

September 2024

Gorkem Yigit

The telecoms industry is at a pivotal point and operators must make important decisions that will have far-reaching consequences. Some operators will choose to become utility-like entities and will provide commoditised infrastructure in a cost-competitive manner. However, others will develop new business models and platforms that offer more differentiated, monetisable network connectivity and adjacent services to pursue new revenue opportunities, particularly in enterprise markets, but also potentially for pure service providers that do not own their networks.

In this article, we discuss the role of the network-as-a-service (NaaS) concept in this evolving market landscape and provide a definition. We also review the features and characteristics of NaaS as covered in Analysys Mason's *NaaS Platforms and Infrastructure* research programme.

What is NaaS?

The industry needs to find ways to offer advanced and monetisable network services. Traditional networks and operations fall short of achieving these objectives, and existing business models offer limited growth potential and carry the risk of finding themselves under pressure with reduced margins and declining influence in the value chain. Networks should become 'first-class citizens' in the new cloud and AI-centric world, rather than being an impediment to service agility and innovation. This transformation will require networks to be rearchitected as a programmable, intelligent fabric that can meet diverse connectivity needs and can be exposed and consumed with a cloud-like experience, similar to how IT infrastructure and services are consumed in the public cloud. Converging this network fabric with related value-added services on a single platform and delivering the services on-demand with consumption-based models is the foundation for what the industry is envisioning as NaaS.

The concept of NaaS is not new, but there is not yet an industry-wide consensus on its definition, main principles, and architectural components. MEF is one of the leading initiatives that is working on this. Our view of NaaS aligns with MEF's definition but extends beyond that to include a broader scope of network APIs for programmability and monetisation.

We define NaaS as the next-generation network services platform that has the following main characteristics and features.

- **Any-to-any connectivity** that enables enterprises and developers to connect their distributed applications, users and branches across data centres, public clouds and locations using a variety of underlay networks (for example, Layers 1, 2 and 3) and overlay networks (for example, multi-cloud routing, Layer 7 application layer networking) using a single platform with end-to-end service-level agreements (SLAs).

- **Self-service model** that provides on-demand, automated provisioning, configuration and up-and-down scaling of connectivity and network services.

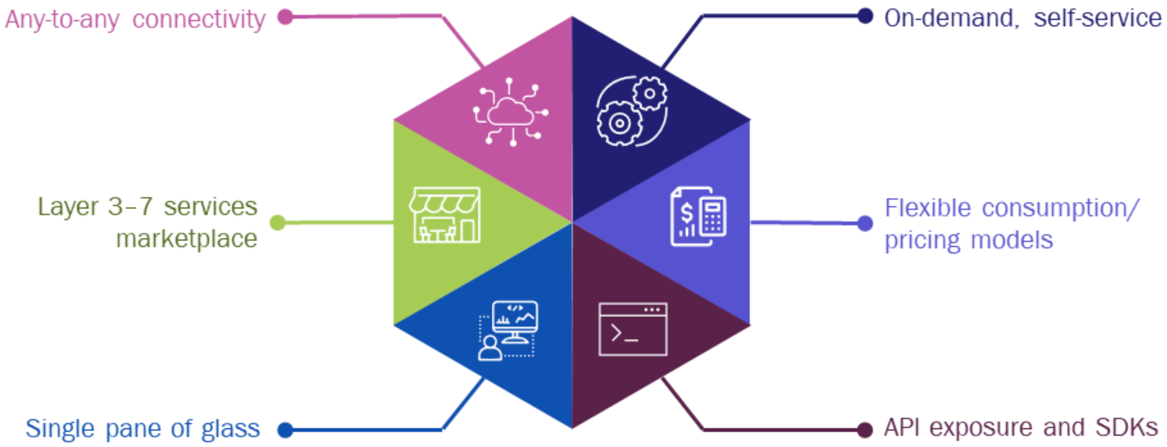
- **'Single pane of glass' management and visibility** of the services that are delivered from the NaaS platform, underpinned by observability, assurance and security capabilities.

- **Flexible commercial/pricing models** for connectivity and related services, such as cloud-like consumption-based pricing (per user, bandwidth or use case) in an opex model.

- **Exposure of network and platform capabilities** through open APIs, including industry-standard APIs such as those created by CAMARA or MEF, and software development kits (SDKs) for developers and DevOps/CloudOps teams to enable programmability.

- **Value-added services marketplace** that offers various Layer 3–7 services, such as security, SD-WAN, remote access, cloud/co-location and unified communications (UC) services, which are either from a partner ecosystem and/or developed in-house.

Figure 1: Characteristics and features of NaaS platforms



Source: Analysys Mason

What is driving the demand for NaaS?

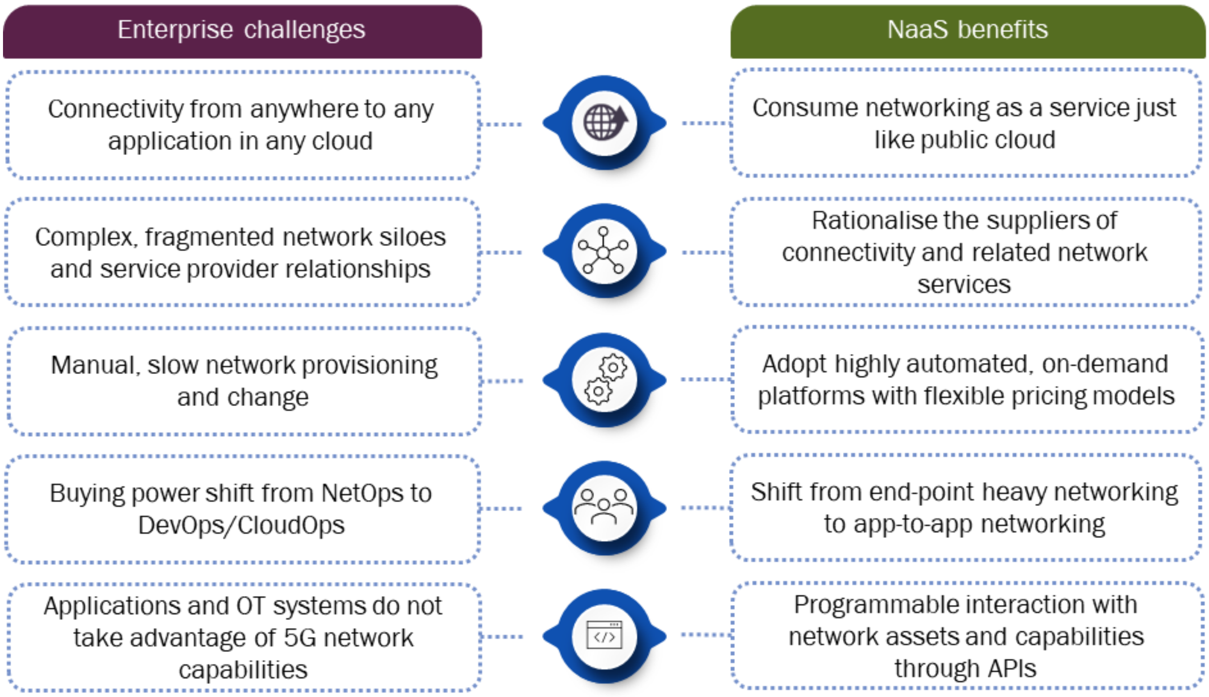
Enterprises' networking requirements are changing rapidly with the adoption of public cloud, SaaS and, more recently, AI (Figure 2). The increasingly distributed nature of enterprise cloud-native applications and workloads across a growing number of public, SaaS and edge clouds, in addition to their on-premises data centres and geographically dispersed users and locations, requires reliable, secure and programmable connectivity between these environments. However, traditional B2B connectivity and security services are highly fragmented, forcing enterprises and their service providers to manually stitch together a complex set of networks and services. As a result, network provisioning is slow and change processes can take several months compared to minutes or hours for compute and storage resources in the cloud. Consequently, enterprises are increasingly demanding networks as a managed service and seeking simple, on-demand provisioning of network and Layers 4–7 services in a consistent and flexible manner, using as few service providers as possible.

Another important trend is the shift in power between buyer personas within the enterprises. Many new network buyer personas have emerged (CloudOps, DevOps, SecOps) in addition to traditional NetOps and they demand cloud-native, application-based secure networking capabilities that integrate with CI/CD pipelines and infrastructure-as-code tools across public clouds and on-premises data centres. As such, enterprises need NaaS platforms that cater to the different needs of various networking buyers/users, through a unified, self-service experience and consistent security and compliance policies.

Beyond connectivity, operator 5G and transport networks contain many features, data and insights that can support the needs of application developers (for example, quality of service and experience (QoS/QoE), security, fraud prevention, digital transactions) and Industry 4.0 use cases such as manufacturing automation, public safety, digital twin-driven supply chains and many others. However, traditionally, there has been a gap in effectively exposing these capabilities. To bridge this divide, NaaS provides an opportunity for specific network functionalities and features to be exposed to developers in a simple way, allowing them to be programmed into specific applications and operational technology (OT) business logic and called on-demand through APIs.

Network slicing within 5G networks becomes crucial in the NaaS context. Network slicing is still at an early stage and faces several commercial and technical challenges, but it has the potential to enrich NaaS propositions by allowing enterprises and developers to create multiple virtual networks on a single physical infrastructure with each slice tailored to specific application requirements, offering dedicated resources, enhanced security and optimised performance. The use of APIs for programmatic slicing enhances NaaS platforms, providing the on-demand, application-based network provisioning with more granular control and flexibility that enterprises want.

Figure 2: Enterprise networking challenges and how NaaS can address these challenges



Enterprise challenges	NaaS benefits
Connectivity from anywhere to any application in any cloud	Consume networking as a service just like public cloud
Complex, fragmented network siloes and service provider relationships	Rationalise the suppliers of connectivity and related network services
Manual, slow network provisioning and change	Adopt highly automated, on-demand platforms with flexible pricing models
Buying power shift from NetOps to DevOps/CloudOps	Shift from end-point heavy networking to app-to-app networking
Applications and OT systems do not take advantage of 5G network capabilities	Programmable interaction with network assets and capabilities through APIs

Source: Analysys Mason

What does NaaS architecture look like?

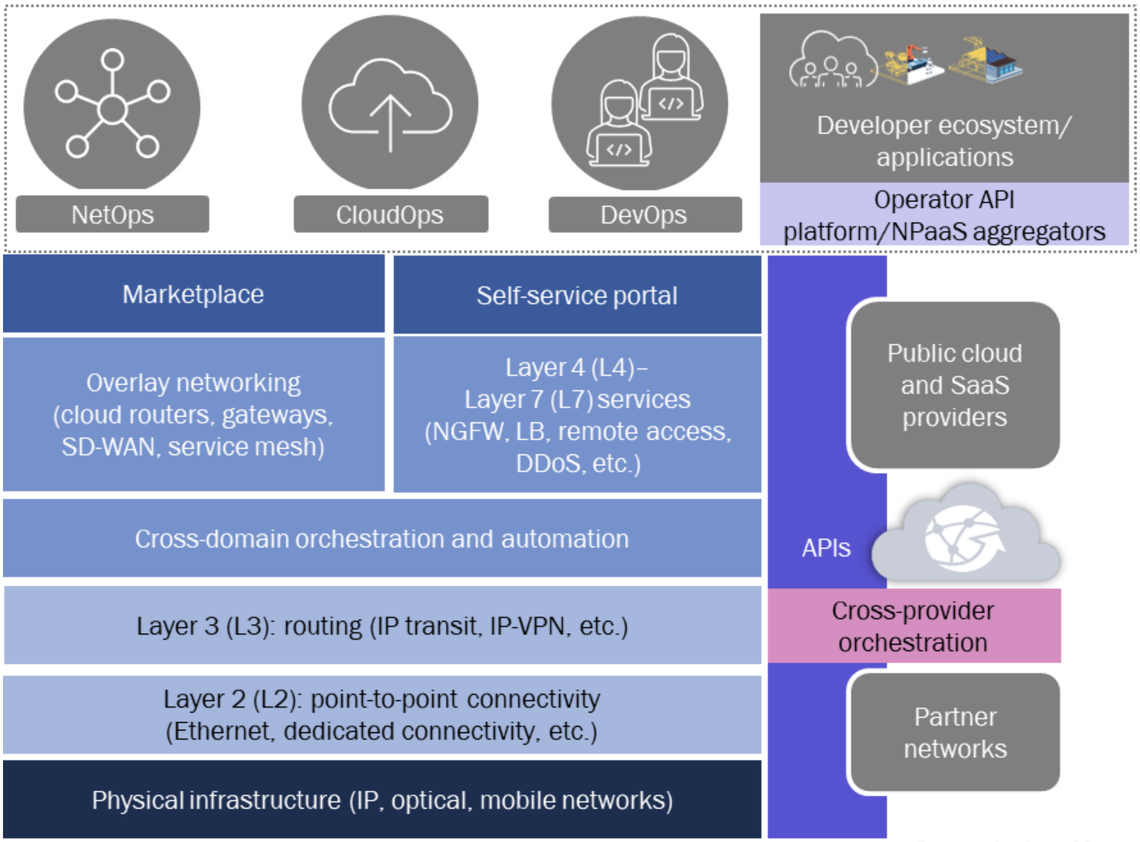
This evolving enterprise connectivity landscape, and the new application and developer requirements, need to be addressed by NaaS platforms. An ideal, holistic NaaS platform architecture to achieve this goal should consist of the following three service layers (Figure 3).

- **Software-defined, highly automated underlay networks.** Underlay networks (Layers 1, 2 and 3) remain an essential part of offering flexible, on-demand connectivity services (dedicated cloud connectivity, private Internet, Ethernet, IP-VPN, data centre interconnect) with advanced SLA, QoS and privacy/sovereignty. The traditional mode of delivering these services resulted in flat or declining revenue. NaaS gives operators an opportunity to defend and potentially boost their revenue by better positioning these underlay network services as a lynchpin for growth areas such as cloud and data-centre connectivity. Integration and orchestration of partner service providers' underlay networks using industry-standard APIs are also becoming important in overcoming geographical footprint constraints to support this goal.

- **Cloud-native overlay networks.** Distributed applications and multi-cloud connectivity are driving the demand for cloud-native, application-centric networking, which is estimated to become a USD4.3 billion market by 2028. This demand cannot be addressed with underlay networks. NaaS platforms should provide a full suite of network-agnostic, Layer 3–7 overlay solutions (cloud routing, application networking, security, optimisation) that are necessary for intra- and cross-cloud connectivity, backed by the SLA, QoS, security and privacy guarantees of underlay networks.

- **APIs.** NaaS platforms should be built with a variety of internal and external API layers spanning north-south APIs to support operational automation, east-west APIs for orchestrating services between service providers and external, customer-facing APIs, including industry-standard APIs, such as those created by CAMARA, as well as proprietary ones, to aggregate, abstract and expose fixed and mobile network assets and capabilities to enterprises and developers.

Figure 3: Overview of NaaS architecture


NetOps
CloudOps
DevOps
Developer ecosystem/ applications
Operator API platform/NPaaS aggregators
Marketplace
Self-service portal
Overlay networking (cloud routers, gateways, SD-WAN, service mesh)
Layer 4 (L4)– Layer 7 (L7) services (NGFW, LB, remote access, DDoS, etc.)
Cross-domain orchestration and automation
Layer 3 (L3): routing (IP transit, IP-VPN, etc.)
Layer 2 (L2): point-to-point connectivity (Ethernet, dedicated connectivity, etc.)
Physical infrastructure (IP, optical, mobile networks)
APIs
Public cloud and SaaS providers
Cross-provider orchestration
Partner networks

Source: Analysys Mason

What is the NaaS value chain and who are the main players?

NaaS is reshaping the enterprise connectivity value chain, with a variety of players simultaneously competing and partnering with each other. The market is formed of a mix of service providers with various underlay and overlay network capabilities and focus areas (Figure 4). These providers include telecoms operators, specialised B2B connectivity providers, software-defined cloud interconnect (SDCI) players, co-location/internet exchange (IX) providers, cloud-native networking software providers and public cloud providers (PCPs), which have become a key part of this landscape with their global backbones and managed WAN services.

Figure 4: Categories of NaaS providers

Categories of NaaS providers	Examples
Telecoms operators	AT&T, BT, Deutsche Telekom, Orange, Telefónica, Verizon and Vodafone
Specialised B2B connectivity providers	BSO, Colt, Lumen and Zayo
SDCIs	Alkira, Console Connect, Intercloud, Megaport and Packet Fabric
Co-location/internet exchange (IX) providers	Core Site, Digital Realty and Equinix
Cloud-native networking software providers	Aviatrix, F5, IBM and Prosimo
Multi-cloud SD-WAN managed service providers	Apcela, Aryaka, Cato Networks,
Public cloud providers	AWS, Azure, Google and Oracle

Source: Analysys Mason

NaaS is a natural evolution for telecoms operators because they have large network assets and existing customer relationships. However, their general lack of automation, flexibility and programmability due to their high level of fragmentation and legacy network technologies puts them at a disadvantage against modern alternative service providers that have built highly automated and agile solutions with NaaS in mind from the outset. Operators have several strategies available to overcome these challenges including:

- building new NaaS infrastructure and platforms from scratch, such as BT's Global Fabric
- undertaking NaaS-driven transformations of the existing networks, as demonstrated by Orange in its Evolution Platform and DT's Software Defined Business Hub
- acquiring a NaaS platform, either procuring a white-label solution (a Tier 1 US operator and F5) or purchasing/investing in an existing service provider or start-up to acquire the solution, IP and staff (for example, Deutsche Telekom and Teridion, and PCCW and Console Connect)
- or simply reselling a partner's NaaS platform solution.

Operators also have an opportunity to differentiate their NaaS propositions by combining their private networks, 5G standalone (SA) core and edge networks and exposing them through APIs to enable the advanced use cases discussed in the previous section that other NaaS providers cannot offer.

From the supply side, NaaS provides a significant opportunity for technology vendors. Several vendors, such as Cisco, Huawei and Nokia, as well as the newly combined HPE/Juniper, are capable of assembling end-to-end NaaS platforms for service providers together with ecosystem partners. Challenger vendors such as Arrcus and DriveNets also have an opportunity to provide open, disaggregated solutions to support NaaS-centric infrastructure transformations. Automation and AI will be embedded parts of NaaS platforms, generating demand for network automation and orchestration solutions from Amdocs, Ciena/Blue Planet and Netcracker as well as cloud-native infrastructure and automation providers such as Red Hat, VMware and PCPs. NaaS service providers will need to partner with L4–7 application providers such as Checkpoint, F5, Palo Alto and others to offer value-added services marketplaces. Finally, Ericsson/Vonage, Nokia and PCPs will play an important role in building the network API service platform layers.

Overall, the NaaS value chain is crowded and fragmented, and no single service provider or vendor fully addresses the complete NaaS requirements yet. While these players continue to expand their capabilities organically and partner with each other to fill the gaps (facilitated by increasing standardisation), the NaaS market is poised for consolidation and simplification, at the service provider and technology vendor layers, to achieve better service integration and scale to provide more comprehensive and unified services.

Gorkem Yigit is a Research Director and heads Analysys Mason's *NaaS Platforms and Infrastructure* and *Cloud and AI infrastructure* research and insights programmes. The NaaS Platforms and Infrastructure programme tracks the evolving and complex value chain of NaaS; examines service provider and vendor strategies, and NaaS architectural building block technologies and market trends; and assesses the implications and opportunities for service providers, technology suppliers, regulators and financial institutions.