LTIMindtree

Whitepaper

Network-as-a-Service
Empowering Businesses and Networks

Contents

Abstract

Organizations today face continuous cost pressures as they strive to adapt to the digital era and evolving nature of service consumption methods. Moreover, unexpected investments due to rapid technological advancements compel organizations to frequently revise their technology adoption roadmaps. As the backbone of IT, networks must be transformed to provide secure, agile, automated, and reliable services through software-defined infrastructure. With the growing adoption of artificial intelligence (AI), it is essential to invest heavily in the infrastructure, especially in network capabilities. Many organizations are opting for public cloud services to avoid high upfront costs and enable faster integration. Network infrastructure can also be leveraged with similar agility, flexibility, and ease of management as cloud services.

The Network-as-a-Service (NaaS) market is experiencing significant demand among enterprises who value flexibility, on-demand scalability, and simplified management. Organizations across industry verticals, especially in finance, healthcare, and manufacturing, are increasingly moving to subscription-based NaaS models to reduce the overhead of traditional infrastructure refresh and take advantage of advanced software-defined networking capabilities.

The journey of NaaS commenced with the provision of on-demand wide area network (WAN), enabling enterprises to adjust their bandwidth according to application requirements. Since then, NaaS has significantly evolved to encompass software-defined networks, wired and wireless local area networks (LAN), Software-defined Wide Area Network (SD-WAN), and management platforms. Presently, NaaS allows organizations to utilize network infrastructure—including hardware, software, and services—via flexible subscription-based models. This approach enables businesses to stay aligned with evolving demands and adopt robust digital AI services without being restricted by conventional network procurement methods.

For organizations with a global presence, investments and spend management must cover country-wise budgets, different currencies, expense forecasts, and asset tracking. If there are regional contracts, financial management becomes even more complex. Towards this, NaaS offerings are often designed to address not only technology adoption and operations-related challenges but also to simplify financial management. The key solution areas addressed by NaaS models are listed below.

- Technology currency and digital service readiness
- Right-sizing network infrastructure with a cloud-first and security-first approach
- Shifting enterprise spends from CAPEX to OPEX, covering hardware, software, and services
- Simplified monthly billing catalogues with centralized/ regional billing flexibility
- Predictable cash flows and transformation roadmaps

Introduction

In today's era of digital transformation, businesses are increasingly relying on cloud services to enhance agility, scalability, and cost-efficiency. Organizations are striving to keep pace with technological advancements, achieve faster time-to-market, and drive cost optimization and operational efficiency. With the integration of AI-ML and the adoption of Gen AI, the investment required for the underlying network infrastructure has increased significantly. Also, the service consumption patterns have changed in areas like hybrid/ distributed workforce, digital industry 4.0 initiatives, online retail and delivery tracking, and cloud user repositories. These challenges have led to a substantial rise in the demand for as-a-service models. Network-as-a-Service (NaaS) is an emerging concept that aligns with these objectives by offering network infrastructure on a subscription-based model. This enables organizations to operate their networks without upfront investments in buying, building, or maintaining network infrastructure.

While the NaaS offering is subscription-based and often driven by a Remuneration Unit (RU) catalogue for quicker adoption, it is important to understand the construct, key considerations, network transformation, adoption roadmap, geographic coverage, asset ownership, and contract novation involved in developing the appropriate strategy for a given opportunity. This whitepaper examines the definition, benefits, and use cases of NaaS, along with its associated challenges.

Insights from industry analysts

Enterprises are adopting NaaS to buy, deploy, and manage their networks more efficiently. Independent sources like IDC, Kearney, and 650 Group confirm the rising demand for NaaS in recent studies.

IDC

It's an exciting time in the enterprise NaaS market.

Market awareness and the use of NaaS is expanding, driving its ability to deliver financial benefits such as predictable costs and easier budgeting.[1]

Kearney

NaaS' future is bright.

NaaS gives customers a seamless network experience in return for monthly payments, while eliminating the worry of service-related issues and frequent, costly capital expense (capex) upgrades.[2]

650 Group

NaaS is a natural progression.

We see heightened demand for different consumption models throughout the differing networks of ethernet switching, wireless LAN, and SD-WAN, especially as customers look towards subscription models.[3]

As per Gartner's 2025 Strategic Roadmap for Enterprise Networking, "For new infrastructure or service contracts, it is important to evaluate usage-based/ NaaS alternatives for cost and flexibility advantages. By 2028, on-premises NaaS will be adopted by 15% of all enterprises, which is an increase from less than 2% in 2023."4

Comprehensive value of NaaS

NaaS is a cloud-like commercial model that enables customers to subscribe to networking services from a predefined RU catalogue. It allows customers to utilize network services, including hardware, licenses, and managed services, through a subscription. Often driven by technology refresh initiatives, NaaS also includes transformation services to ensure tech currency and serve the needs of digital initiatives. Billing for these services can occur monthly / quarterly, either centrally or regionally, based on the terms of the contract. It encompasses a range of services, including Software-defined Local Area Network (SD-LAN), WAN Connectivity, SD-WAN, Secure Access Service Edge (SASE), Infrastructure Security, Network Access Control (NAC), Observability, and Management Services.

In the NaaS model, the hardware is dedicated solely to a specific customer and particular sites, in contrast to the cloud's as-a-service model, where the underlying platforms are designed for shared use. In the NaaS model, assets are leased to customers for a specified duration instead of being owned by them. This model encompasses asset deployment, ongoing support services, and metering and billing activities, all bundled under the NaaS contract. NaaS provides customers with comprehensive visibility into their network services through a dedicated portal, while the service partner maintains end-to-end ownership and control.

Driving business agility: The case for NaaS adoption

Organizations are adopting NaaS for increased financial and operational flexibility. Rather than making significant upfront investments, they can use infrastructure services as needed and pay only for what they use. This method ensures that infrastructure stays in line with technological and business advancements.

Technology currency: Rapid changes in technology make network equipment obsolete, often unable to support modern IT services. NaaS subscription models allow organizations to stay current with quick tech refresh cycles while reducing security and cost concerns linked to outdated hardware. Though repurposing and disposal are expensive, sustainable reuse and retirement in NaaS help meet sustainability goals efficiently.

Flexibility and agility: NaaS allows organizations to avoid upfront capital investments and complex budget approvals, deploying technology as needed. It offers predictable costs and pay-as-you-go options, helping organizations adapt to rapid changes and manage limited capital. NaaS offers the capability to meet business requirements by launching new services and capabilities more quickly, particularly when network planning cycles are shortened and organizations need to adapt rapidly to market changes or take advantage of new opportunities.

Optimized cost: In addition to annual capital expenditure challenges associated with adopting new technologies, organizations also encounter constraints related to return on investment from their existing investments. Towards this, NaaS offers simplified contracts and predictable cash flows, enabling organizations to avoid substantial upfront investments and eliminate expenses related to maintenance and frequent asset refreshes.

Predictable network performance: NaaS deployments tackle performance and security risks through proactive advisory and management capabilities. These often include AI-ops-driven insights, helping organizations enhance security and performance with the latest features, functionalities, and configurations. This proactive approach addresses potential problems before they cause outages or performance degradation.

Simplified operations: NaaS offerings typically feature centralized, cloud-based tools designed to simplify network management, enhance visibility, and ensure efficient policy governance. Organizations can prioritize strategic initiatives by consolidating network contracts and streamlining metering and billing processes rather than allocating extensive resources to service and contract management.

From evaluation to integration:
A pragmatic approach to NaaS adoption

While every organization relies on network infrastructure to support its business services, many have made significant investments in this area only recently. Given various network domains (LAN, WAN, and DC Networks) and multiple deployment models, it is crucial for organizations to evaluate the key characteristics of NaaS and determine its suitability for their specific environment.

Entirety: A NaaS subscription model should include hardware, software licenses, and associated managed services to avoid split responsibilities and multiple service ownerships. For instance, physical circuits and SDWAN software overlays can be offered as a service, while the on-premises Customer Premises Equipment device is provided by the customer. Such arrangements would result in differing contract management and shared ownership between parties for the same WAN service.

Predictive costs: The subscription should offer insights into consumption patterns, forecasts, and the capacity to expand or scale services as needed. The commercial structure should include an RU catalogue with a detailed line-item breakdown for easy consumption, anticipating future expenditures, and predicting cash flows.

Global coverage: Network (LAN and WAN) infrastructures often extend across various countries. Each region or country uses different currencies, price lists, and regulations. A partner's ability to offer global coverage with centralized or local billing capabilities is crucial for the successful adoption of NaaS. A contract structure should allow organizations to subscribe to network components at prices and currencies specific to each country.

Cloud management: A fundamental component of NaaS is managed services, which require a robust, scalable, and centralized management platform. This platform can also facilitate application programming interface (API) integration with IT Service Management systems for streamlined service-level agreements (SLA) and contract management. While offering this management platform as an on-premises dedicated solution is possible, a cloud-based management tool enables faster deployment, enhanced scalability, and effortless decommissioning at contract termination.

Integrated security: With an increasing network attack surface and initiatives like Zero Trust Network Access (ZTNA), security must be a fundamental aspect of any transformative initiative. As part of the technology update through the NaaS model, organizations should consider consolidating multiple solutions and bundling network security components under one subscription. This approach can facilitate better integration between NetOps and SecOps, resulting in easier management of security policies, better lifecycle management, increased security patching, and improved compliance.

Automation and AI-ops: In the modern network landscape, features and functionalities have evolved to include automation and artificial intelligence capabilities. Next-generation network solutions should be able to automate network operations, such as event correlation, anomaly detection, and proactive alerting. Predictive analysis and self-service automation services should aim to enhance the user experience. The NaaS model should consider this as a key measurable parameter.

While considering these key parameters, organizations are advised to adopt NaaS incrementally. It is prudent to maintain a co-existence of traditional and NaaS infrastructure, avoiding the replacement of fully functional existing systems. Strategically adopting NaaS models during asset refresh cycles is recommended. Organizations should integrate NaaS infrastructure as an additional vendor service within their ITSM platform and gradually phase out traditional infrastructure along with its associated service metrics.

Strategic readiness:
Key considerations before embracing NaaS

Understanding and addressing the barriers in traditional network services is essential for successful NaaS adoption.

Significant recent investment: An up-to-date Configuration Management DB with a detailed end-of-life analysis is essential to define the NaaS adoption strategy. If a significant percentage of devices are new, then the NaaS model may not be advantageous. In some scenarios, asset takeover can be considered, but organizations need to provide appropriate documents justifying the netbook value (NBV) to maximize the benefits of such arrangements.

Compatibility issues: The coexistence of traditional and NaaS infrastructure must be evaluated regarding interoperability challenges. Compatibility with new SDWAN infrastructures can be problematic, especially for existing SDWAN setups. Depending on the lifecycle of the current SDWAN deployment, organizations may choose to wait for the refresh cycle or transition to a new NaaS model. For LAN infrastructure, it is recommended to transition site-by-site to the new NaaS infrastructure.

Security concerns: Existing security controls and operating models may need to be reviewed under the new NaaS framework, which includes solutions like NAC, on-premises firewalls, and SASE. Organizations should clearly outline data security and regulatory compliance requirements within the NaaS contract and adopt a collaborative working model with the new provider.

Relinquishment of control: While NaaS provides organizations with comprehensive visibility into the network services delivered, the actual control over the infrastructure will transition to the provider. Despite the cloud-like nature of NaaS , some organizations are hesitant to relinquish control over assets located on their premises. It is essential that NaaS contracts clearly define the appropriate service governance framework to address these concerns.

Geographical challenges: The ever-changing political landscape, including taxes, duties, and embargoes, makes it difficult to include certain countries or regions in the NaaS contract. Additionally, the availability of providers worldwide is crucial for NaaS' success. It is recommended to outline country-specific coverage along with the anticipated spending. In some non-business friendly countries, opting for Capex may be more practical.

The NaaS marketplace at a glance:
Choosing the right fit

Today, various Original Equipment Manufacturers (OEM), traditional telecommunications companies, and managed network service providers/ Global System Integrators (GSI) offer NaaS services in multiple forms. Though there are numerous options available in the market, it can be challenging to identify the techno-commercially appropriate solution for a specific requirement. The table below provides a summarized overview of different NaaS services provided in the market.

Network OEMs

- Vendor-specific product offering. No coverage for other vendor products or WAN circuits
- Clear definition of product catalogues
- Limited direct coverage, mostly through GSI partners
- Support services that are limited to remote delivery models.
- Device uptime-related SLA-focused contracts
- Often built on a shared services model
- High reliance on third-party vendors for deployment
- Rigid legal and contract terms

Telecom Service Providers

- Multi-vendor product offering but tied to own circuit subscription
- Strong global coverage with flexible billing options
- Mostly per-site-based contracts with fixed duration
- Strong in SDWAN and circuits under NaaS models
- Lack of enterprise LAN and DC LAN delivery, leading to subcontracting such services
- Often built on a shared services model
- Costlier in enterprise LAN contracts when compared to SDWAN.

Managed Network Service Providers (GSI)

- Flexibility in providing multi-vendor and multi telco offerings
- Purpose-fit NaaS contract with clear definition of RU catalogues
- Transparency of service elements like hardware, software and services.
- Option for shared/ dedicated service delivery models
- Service-oriented delivery model with API-based ITSM integrations
- End-to-end ownership of network services, covering centralized monitoring, management and onsite support.

In network services, there is no universal model as it must be tailored to the specific needs of every organization. Managed network services from GSIs can customize solutions from single or multiple vendors and package them as a service for easier consumption. For WAN circuits and SDWAN-bundled requirements, telecom NaaS offerings may present a better commercial proposition. Organizations should consider these aspects when deciding on their NaaS strategy and evaluating providers.

Conclusion

NaaS represents a significant shift in how organizations consume and manage network infrastructure. By offering scalable, cost-effective, and secure networking solutions, NaaS enables businesses to focus on their core operations while leveraging advanced network capabilities. Despite its challenges, the benefits of NaaS make it a compelling choice for modern enterprises seeking to enhance their network agility and performance.

NaaS facilitates the rapid adoption of technology, addresses evolving business dynamics, and enhances user experience without requiring substantial upfront investment. The following is a summary of NaaS' advantages:

- Delivers faster network deployment of new features and functionalities.
- Reduces significant capital investments needed for extensive deployments with a subscription-based model.
- Streamlines and simplifies network service contracts in accordance with country-specific regulations.
- Ensures asset lite business operations and contributes to an organization's sustainability goals.
- Simplifies operational complexity with a model tailored to your needs.
- Provides consistent monitoring for performance and security, reducing the burden for resource-constrained organizations.
- Offers proactive management capabilities, with access to highly skilled networking experts assigned specifically to the account.

References

- IDC White Paper sponsored by HPE, NaaS State of the Market: As Adoption Continues, Benefits of as a Service Models Crystalize Doc#US50530723, April 2023[1]
- Kearney, "Agile networking: how NaaS is challenging the traditional enterprise networking market," Sridhar Narasimhan, Tanya Khera, Shuhei Umemoto, August 23, 2023[2]
- 650 Group, "650 Group Launches New Research Report Series Focused on Network-as-a-Service," March 23, 2022[3]
- Gartner's 2025 Strategic Roadmap for Enterprise Networking[4]

About the author

Ravi Shankar Ganesan

Managing Principal Architect

Ravi is a seasoned architect and network practice leader with over 25 years of experience in designing, securing, and scaling network and security infrastructure for Fortune 500 companies and global organizations. While his expertise spans commercial modeling, business case analysis, engineering management, Ravi is adept at delivering comprehensive development, market validation, and enterprise network transformation strategies.