The practitioner's guide to NaaS

HPE aruba networking

What Are CapEx and OpEx
There are different ways of accounting and paying for business expenses—the most common of which are capital expenditures (CapEx) and operating expenses (OpEx). Internal accounting rules may vary, but in general, capital expenditures are major purchases that a company makes, which are used over the long term and paid for in one lump sum at time of purchase. Operating expenses, on the other hand, are the day-to-day expenses that a company incurs to keep its business running and paid for as they are incurred.

- Examples of CapEx include physical assets, such as buildings, equipment, machinery, and vehicles.
- Examples of OpEx include employee salaries, rent, utilities, and property taxes.

Overview

Many organizations are considering some form of network as a service (NaaS) to address cost, staffing, and technology needs. A predictable and flexible monthly bill with third party management is attractive, especially for C-level executives and application and business managers who want to move to a NaaS model.

Business requirements, not technology, increasingly drive IT decisions. That said, businesses need help sorting out and understanding various NaaS models and claims, especially when they portray a "simple and easy" solution without detailing the realities of delivering a reliable service. Implementing a new network solution is not trivial, even in a simplified model where the intricacies and nuances of deploying a network are disguised in a "one size fits all" story.

NaaS provides an opportunity for the technical team to partner with and inform the business about implementing a NaaS network solution that delivers the right business outcomes.

Developing a NaaS strategy

While NaaS is typically defined as a monthly payment for a network that is managed by a third party, most organization's NaaS needs are much broader than that. To reach the right NaaS outcome, organizations should consider 6 NaaS dimensions, which will define the most effective NaaS solution for their unique needs. As the networking team and the business work together to refine their needs, a set of requirements begins to emerge that can form the basis of an RFI or RFP.

We call this robust, flexible NaaS solution Agile NaaS from HPE Aruba Networking. The following diagram explains the dimensions and choices provided by Agile NaaS.

6 Key dimensions of Agile NaaS

CAPEX	FINANCIAL MODEL	OPEX
SELF-MANAGED	OPERATIONAL MODEL	THIRD-PARTY MANAGED
INCREMENTAL	TECHNOLOGY ADOPTION	FULL REFRESH
ON PREMISES	DEPLOYMENT MODEL	PUBLIC CLOUD
CONSISTENT	DEMAND PROFILE	PEAKS AND VALLEYS
COST FOCUSED	NETWORK FOUNDATION	PERFORMANCE FOCUSED



Some of these dimensions are primarily business-related, but others involve a deeper technical evaluation to arrive at a conclusion. This is where the technology team can explain the implications of various NaaS approaches.

Key NaaS factors

At its foundation, NaaS is about delivering connectivity for a monthly fee—and based on the NaaS strategy, it can be managed internally or by a third-party. With either management strategy, networking professionals know that meeting business objectives and user expectations involves an interconnected set of network technologies that determine if a NaaS solution will be successful.

Maturity. Networks vary by topology, configuration, scale, and environment. A turnkey NaaS solution must demonstrate that it can work across any combination of these variables, which only comes with many years of successful real-world exposure.

Performance. User experiences and business results are directly related to the network's ability to provide sufficient connectivity and performance. What that means varies over time based on the number of connected devices and their corresponding workloads. A network must be capable of handling both the steady state and unexpected peak demand and grow with the organization.

Reliability. Reliability comes from two perspectives. The first is how likely is it to fail? Most networking products start with the same basic components, but hardware reliability comes from a design objective that prioritizes uptime across many years of operation (99.999 availability) in all operating environments, extensive QA cycles that reflect countless different network demographics, and Wi-Fi Alliance certification that validates the product.

User experience. Connectivity alone is not enough to support the business, and great user experience extends beyond the hardware. Wireless connectivity, in particular, requires extensive experience in making sure the Wi-Fi signal is available and optimized for users as they roam while using a variety of devices. Software and analytics must work in conjunction with the hardware to continuously evaluate and adjust Wi-Fi settings to properly support users and devices, such as sensors and AV equipment. Automated tools that determine user satisfaction from the point of connection to the application ensure that SLA's are being met.

Security. Zero Trust and SASE frameworks start with identity-based access control built into the network. Authenticating, authorizing, segmenting, and monitoring user and device traffic is a core function of the network and requires both software and hardware to define policies and enforce access privileges—enforcement that must be done by switches, access points, and SD-WAN gateways and the cloud, not by external third-party devices. In addition, the network must have seamless integration and interoperability with the rest of the security ecosystem to ensure maximum protection.

Analytics and automation. It is tempting to assume that using a third party to help manage the network will solve staffing shortages and skills gaps. In fact, the answer is not about shifting responsibility for manual and inefficient processes; the solution is to leverage the power of analytics and Artificial Intelligence (AI) to reduce the time to plan, deploy, manage, and optimize the network. And, trusted AI that helps manage the network requires data to train the machine learning models. Therefore, it is critical that large volumes and a wide variety of relevant data are continuously collected and stored in an AI data lake to constantly improve the AI results. Small market share players, especially NaaS-only vendors, cannot purchase or synthetically assemble the necessary data lake. Recommendations and insights can be trusted only when they come from a data lake derived from a large customer base that provides data relevant to any network size, topology, and vertical industry.

Balance business needs with network realities

NaaS can sound almost too good to be true to the business manager. Lower costs, flexible consumption, and shifting of responsibility can accelerate digital transformation and lead to new and better business outcomes. However, as this guide illustrates, the networking team can work together with business managers to explain all the implications of a NaaS decision and build a NaaS strategy to focus the discussion and reach agreement on NaaS priorities. After agreeing on a strategy, when and how to implement NaaS will meet everyone's objectives.

Take the NaaS assessment to determine your NaaS profile and find recommendations tailored for you.

Make the right purchase decision.
Contact our presales specialists.

Contact us

a00130189ENW