

Enterprise Campus Networks: The Rise of Network-as-a-Service

RESEARCH BRIEF



Table of Contents

Introduction..... 1

What are Network-as-a-Service (NaaS), Campus NaaS, and Enterprise NaaS? 1

 Demand-Side Drivers2

 Supply-Side Drivers4

Characterizing the Nature of NaaS.....5

 What's in a Name: Half-NaaS versus Full-NaaS?.....6

Major Networking Vendors and NaaS7

 Overview of NaaS Upstarts8

 Join.....8

 Meter.....8

 Nile9

 Ramen Networks9

 Shasta Cloud9

Opportunities for NaaS Vendors 10

Barriers to NaaS Adoption 11

Recommendations for Enterprise IT Teams 12

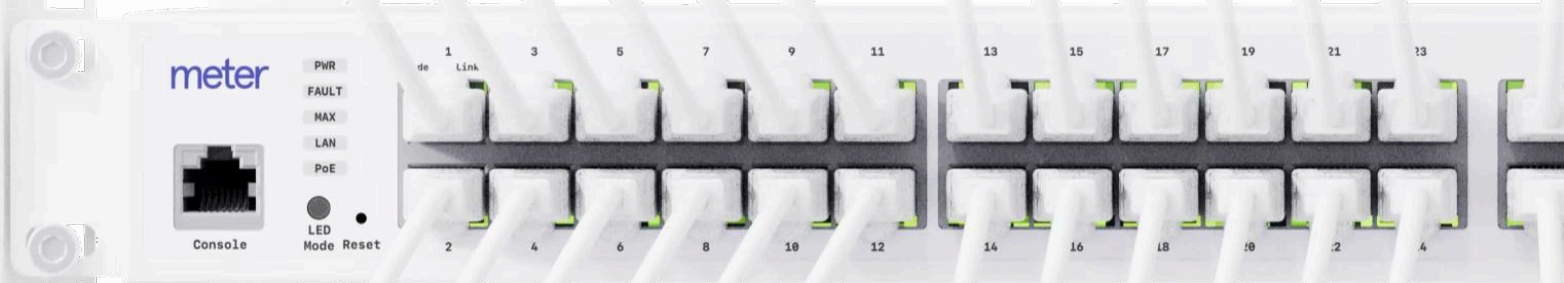
Conclusion..... 13

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorship, please reach out to us at research@avidthink.com.

About AvidThink

AvidThink is a research and analysis firm focused on providing cutting-edge insights into the latest in infrastructure technologies. Formerly SDxCentral’s research group, AvidThink launched as an independent company in October 2018. AvidThink’s coverage includes 5G infrastructure, enterprise networks, private wireless, edge computing, SD-WAN, SASE, SSE, ZTNA, cloud infrastructure, and infrastructure security. Our clients range from Fortune 500 enterprises and hyperscalers to tier-1 communications service providers, fast-growing unicorns, and innovative startups. AvidThink’s research has been quoted by Forbes, the Wall Street Journal, Light Reading, Fierce Networks, Mobile World Live, and other major publications. Visit AvidThink at avidthink.com.

meter



Internet infrastructure for the enterprise

Fully-managed secure connectivity
with zero capital costs.

 meter.com





Cloudifying Branch and Campus LANs

Let Join replace your traditional networks with cutting-edge hardware, implement Zero Trust security, perform proactive monitoring, and utilize AI-driven operations to provide a modern, reliable network.

<https://joindigital.com/products/naas>

Enterprise Campus Networks: The Rise of Network-as-a-Service (NaaS)

Introduction

Network-as-a-Service (NaaS) has evolved significantly since its inception over a decade ago. Initially, communication service providers (CSPs) used the term to describe on-demand carrier connections. However, with the advent of software-defined networking (SDN), the scope of NaaS has expanded into new domains, gaining considerable traction in enterprise and campus networking.

Enterprise campus environments typically feature Layer 2 and Layer 3 local area networks (LANs) and rely heavily on wireless (Wi-Fi) connections. Wireless access points (APs) connect to campus Ethernet switches, which also support wired device connections.

In recent years, major networking vendors have adopted the "as-a-service" model that has revolutionized computing and storage. These traditionally hardware-focused companies are transitioning to software-first and cloud-first strategies, aligning with the elastic, consumption-based business models favored by public markets and investors. Some incumbents now offer NaaS directly to customers, while others collaborate with managed services partners (MSPs) to provide financing and services, creating comprehensive NaaS solutions. Meanwhile, new pure-play "as-a-service" networking startups are emerging, ready to challenge established players.

This research brief focuses on NaaS in the context of enterprise campus networks. A subsequent report will address Carrier NaaS. Here, we explore the growing interest in Campus NaaS among enterprise IT leaders and managed service providers, including communication service providers with managed service offerings. Drawing on our research with networking vendors, service providers, and enterprise users, we provide insights into this emerging market and its potential future, aiming to assist you in making informed decisions for your enterprise networking needs.. Your feedback is welcome at research@avidthink.com.

What are Network-as-a-Service (NaaS), Campus NaaS, and Enterprise NaaS?

AvidThink views NaaS as a business model similar to Software-as-a-Service (SaaS). Like SaaS, which spans various solutions from email and productivity tools to customer relationship management and human resources systems, NaaS can be applied to local-area, wide-area, last-mile, middle-mile, and first-mile network offerings. A successful business model requires alignment across pricing, packaging, contractual relationships, solution architecture, and organizational culture. Just as traditional software vendors underwent significant transformations to adopt SaaS, we expect a similar evolution for NaaS, acknowledging that not all traditional vendors will make the transition successfully.

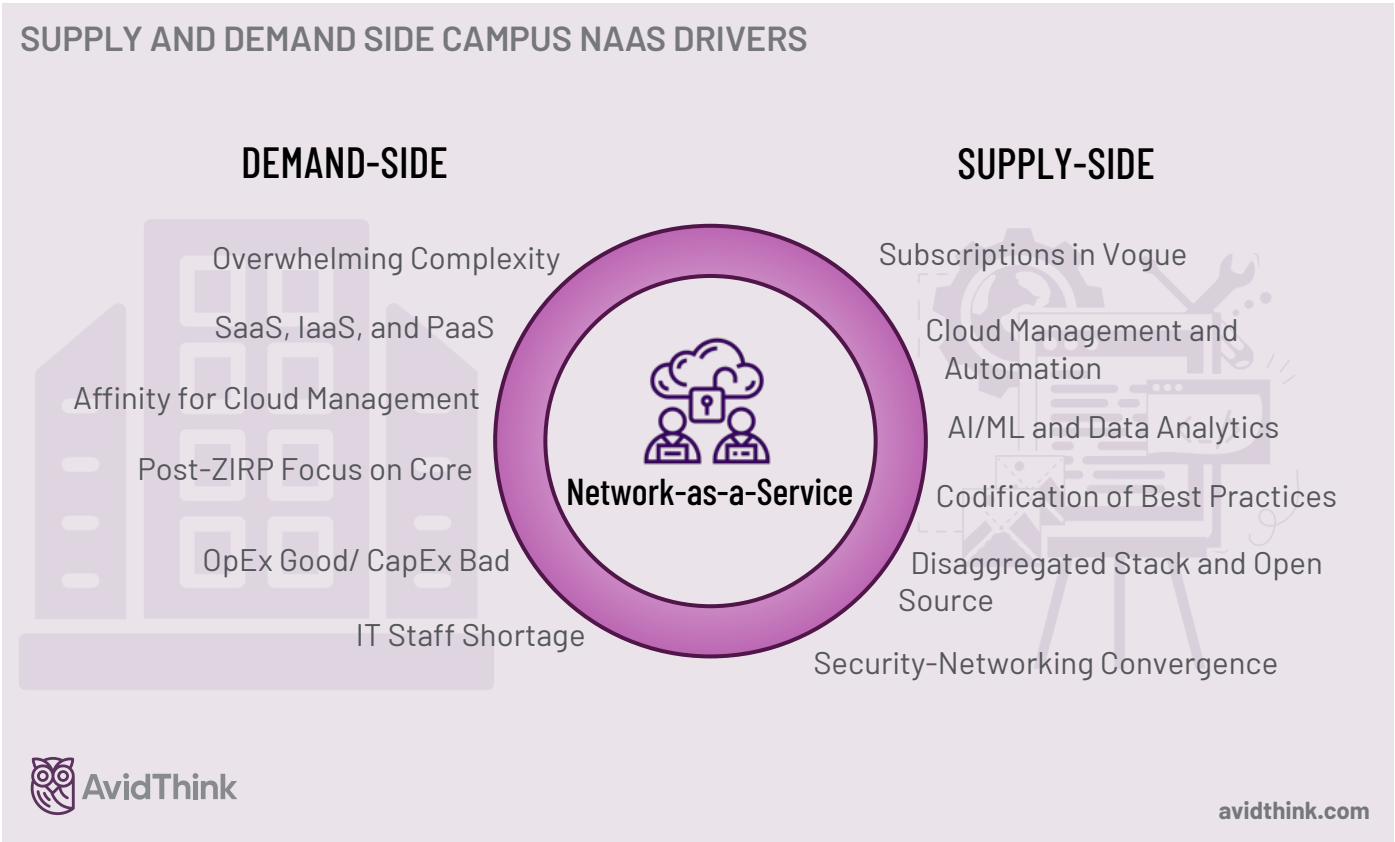
"Campus NaaS" in this report refers to managed network services providing local connectivity in enterprise campus settings, including indoor and outdoor areas and a range of devices from IoT to smartphones. Campus NaaS technologies include Wi-Fi and Ethernet switching, with potential support for 4G LTE, 5G, Bluetooth Low Energy (BLE), and ZigBee for local connectivity and WAN uplinks, particularly in retail or warehousing operations. For this report, "enterprises" include educational institutions, non-profits, and government entities with similar networking needs.

Although Campus NaaS is in its early stages, we anticipate its expansion into Enterprise NaaS, incorporating WAN and security services such as software-defined wide area networking (SD-WAN), firewalls, VPN/zero-trust network access (ZTNA), and other secure access service edge (SASE) solutions. Future expansions may include endpoint security, management, and secure cloud connectivity. Some Campus NaaS providers already offer managed WAN services and integrated security for remote and home offices.

Why Campus NaaS and Why Now?

The campus networking sector has seen little innovation in recent years, aside from cloud management and AI/ML-enhanced network optimization. Best practices in design, deployment, and operations have become standardized, driving enterprises' desire for simplicity and cost consistency, and fostering convergence of networking and security. This environment is ripe for innovation and competition in the Campus NaaS market. Combining enterprise wireless LAN (\$10.8B in 2023¹) and campus switching (~\$25B in 2023²) results in a total market value of \$35B in 2023 (IDC estimate). NaaS, though currently a small segment, is growing rapidly. Dell'Oro projects the market for Campus NaaS and Public Cloud-Managed LAN to reach \$12B by 2028³, with Campus NaaS driving much of this growth.

Why are analysts like IDC, Dell'Oro, and AvidThink tracking the Campus NaaS market? The potential for rapid growth is driven by factors on both the demand and supply sides, which we will examine in detail.



Demand-Side Drivers

Overwhelmed by Complexity

Enterprises are increasingly frustrated by the complexity and perceived nickel-and-diming from their networking vendors. The transition to software-first offerings by major networking vendors has led to convoluted arrays of software modules, often with different licensing schemes, overlapping features, and unclear compatibility with existing hardware. Additionally, various enterprise software and hardware support and maintenance schemes make networking purchases a time-consuming challenge.

¹ Enterprise Wireless LAN Revenues Grew 7.6% in 2023, But Declined Sharply in the Fourth Quarter, IDC Worldwide WLAN Tracker 2024 Mar 7. <https://www.idc.com/getdoc.jsp?containerId=prUS51945024>

² Worldwide Ethernet Switch Market Delivered Robust Growth in 2023 While the Router Market Saw a Slight Decline, IDC Trackers 2024 Mar 8. <https://www.idc.com/getdoc.jsp?containerId=prUS51948824>

³ Campus NaaS and Public Cloud-Managed LAN Revenues to Exceed \$12 B in 2028, Dell'Oro Group <https://www.delloro.com/news/campus-naas-and-public-cloud-managed-lan-revenues-to-exceed-12-b-in-2028/>

Anecdotes from enterprises reveal that even sales teams at top vendors struggle with their software configurators to generate sales quotes. This can lead to incompatible software and hardware modules being sold and shipped, resulting in customer dissatisfaction. Many enterprise customers now seek to avoid separate hardware purchases and the associated complexities of software, maintenance, support, and upgrades. They prefer a single, simplified invoice for their networking needs.

Influence from SaaS, IaaS, and PaaS

The adoption of SaaS was driven by companies' desire to eliminate the burden of installing, upgrading, configuring, maintaining, and patching software. Similarly, Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) gained traction among development teams weary of procuring servers, racking and stacking them in data centers, managing the underlying software and virtualization infrastructure, and scheduling access.

In the same vein, CIOs, IT directors, and managers are seeking alternatives to the overhead associated with procuring, provisioning, managing, and maintaining networks—whether LANs, WANs, inter-datacenter, or multi-cloud networks. Inspired by the success of other utility and consumption-based models, they want similar simplicity in networking. Enterprises desire bundled networking solutions with hardware, software, support, and management, promising business outcomes and service-level agreements without additional headaches.

Post-Pandemic Affinity for Centralized Cloud Management

During the COVID-19 pandemic, many organizations accelerated their cloud initiatives, transitioning from on-premises IT to cloud-hosted, cloud-managed services. This shift amplified the impact of SaaS, IaaS, and PaaS, pushing CIOs to seek cloud-managed controls for remote networking and security. Even as offices reopen post-pandemic, the preference for cloud-managed solutions persists. With a growing number of IT services in the cloud, enterprise networking now prioritizes facilitating Wi-Fi-based LAN connectivity for employees and ensuring robust internet service to cloud-based applications and enterprise data. This alignment reinforces the enterprise preference for a Campus NaaS model.

A Post-ZIRP Focus on Core Capabilities

With the recent end of the zero interest rate policy (ZIRP) era, enterprises face a more challenging business landscape with fewer and more expensive financing options. To navigate this environment, enterprises are focusing on core competencies and outsourcing non-essential IT activities. Campus networking is rarely seen as a strategic differentiator, making Campus NaaS an attractive option. Campus NaaS vendors can leverage economies of scale, specialization, and innovation to manage customer networks more efficiently, passing cost savings and improved service quality to their clients.

Preference for OpEx over CapEx

CFOs and business owners aim to align their revenue with costs, and SaaS models provide a way to achieve this. They look to NaaS for similar benefits, with Pay-As-You-Go (PAYGO) models offering cash outlay over time instead of significant capital expenditures every 36-48 months that require upfront funding and amortization. NaaS can smooth out cash flow, making financial planning easier for businesses. While leasing and vendor or lender financing may offer similar economic advantages, comprehensive NaaS solutions eliminate the complexities of equipment ownership, end-of-lease buyout decisions, ongoing hardware replacements, and partial infrastructure upgrades.

Inability to Recruit and Retain IT Staff

Enterprises are struggling to retain and recruit IT staff, with a particularly acute shortage in cybersecurity positions. Anecdotes from the past few years indicate that finding and retaining seasoned network engineers is becoming increasingly difficult. Moreover, recent college graduates tend to favor software development roles over network engineering roles, believing the former offers higher compensation. This trend has reduced the pool of networking talent. Even enterprises with IT talent prefer to outsource day-to-day network management to allow their IT staff to focus on strategic initiatives instead of routine maintenance or help desk calls.

Supply-Side Drivers

Market Preference for Subscription Revenue

Financial markets today favor predictable revenue streams, and technology companies are now often evaluated using SaaS metrics—customer retention rates, customer acquisition costs (CAC), monthly/annual recurring revenue (MRR/ARR), and customer lifetime value (CLV). Some investors believe that securing customers with annual commitments of one to five years enhances predictability and provides a clearer gauge of company success. This trend is driving incumbent networking vendors to pivot towards NaaS offerings.

Improvements in Cloud Management and Automation

The increased acceptance of cloud-based management for Wi-Fi equipment enables networking vendors to offer greater control of enterprise networks via their cloud platforms, simplifying remote management for vendors and third parties. Networking vendors have also advanced in programmable networks since the early days of SDN, with new networking OS stacks being developed from scratch. These stacks favor an API and model-centric approach over command-line interfaces, facilitating large-scale automation. This significantly lowers network operating costs and reduces the headcount investment needed for vendors to offer NaaS.

Advancements in AI/ML and Data Analytics

Recent breakthroughs in network data analytics and machine learning are making partially autonomous networks possible, aligning well with NaaS principles. The use of generative AI and machine learning can reduce the overhead of operating and troubleshooting networks. Early pilots show a 40-70% reduction in time to root cause identification in complex large carrier networks, and these advantages can be applied to campus networks, which are often less complex.

Mature Deployment and Best Practices Codification

Wi-Fi and Ethernet switching architectures are now well-understood. Experienced networking engineers can plan deployments using floor plans and site survey tools, and seasoned professionals are familiar with best practices for installing structured cabling, predicting dead spots, and placing wireless APs. Many of these practices have been codified into software systems and algorithms, enabling software-assisted planning and management. These capabilities can be leveraged by NaaS vendors for cost-effective and timely remote design and planning, with site surveys used to fine-tune deployments.

Maturity of Disaggregated Stack and Open Source Offers Opportunities for Upstarts

Many merchant silicon vendors, such as Qualcomm, Broadcom, and Mediatek, offer Wi-Fi chipsets for APs. Open software libraries like OpenWRT and dd-wrt provide a foundation for non-incumbent vendors to quickly start the development process. The OpenWiFi and OpenLAN Switching initiatives from the Telecom Infra Project (TIP) offer additional open software stacks and cloud management frameworks. These resources allow new companies to build rapidly, using them as scaffolding until they can improve and replace them or contribute to open-source repositories.

On the Ethernet switching side, options include Open LAN Switching, SONiC as a network operating system, and Free Range Routing (FRR) for Layer 3 routing. Open source security projects like pfSense, OPNSense, OpenVPN, and Wireguard provide starting points for VPN, gateway security, and ZTNA services. These enable NaaS entrants to combine networking and security services for campus LANs, as well as remote, mobile, and home office access.

Security-Networking Convergence Offers Market Expansion

With the increasing enterprise demand to simplify networking and security stacks, NaaS players can develop platforms that integrate both offerings at a single price. NaaS cloud platforms can extend from control and management planes to offering data planes with select SASE services, such as secure web gateways (SWG). Campus gateways for NaaS can be enhanced with next-generation firewalls (NGFW), DNS-based security, and SD-WAN capabilities, allowing for additional revenue streams.

While current NaaS vendors haven't yet bundled in endpoint security, some include VPN remote access clients with zero-trust capabilities in their offerings. It's conceivable that endpoint protection could be added through partnerships or directly from NaaS vendors. Today's SASE vendors have started including endpoint detection and response (EDR) and extended detection and response (XDR). As Campus NaaS evolves into Enterprise NaaS, more security features will converge over the next few years.

Characterizing the Nature of NaaS

We'll soon explore the current Campus NaaS landscape, which includes incumbent networking vendors, each with their own nuanced approach to NaaS, and upstart challengers pushing their pure-play definitions. But before we do that, let's examine the common attributes of NaaS that enterprises expect. Similar to other as-a-service models, enterprise customers look for:

- 1. **Consumption-Based Pricing:** Billing aligns with usage, following a Pay-As-You-Go (PAYGO) model.
- 2. **Quick Provisioning:** Designed for rapid deployment, scaling, testing, and experimentation. While timeframes will vary based on the type of service, NaaS requires hardware installation, meaning "quick" is measured in weeks rather than minutes or hours.
- 3. **Low or No Upfront Capital Expenditure:** Minimal upfront costs for enterprises to use these services, with hardware costs amortized into the subscription fees since NaaS involves dedicated hardware installed on customer premises.
- 4. **Short-Term Commitments:** These services are on-demand or require shorter-term contracts, though many providers offer discounts for upfront credit purchases or longer-term subscriptions. Since on-premises equipment for Campus NaaS cannot be easily re-provisioned for another customer, contracts usually span one to three years, except in office buildings where new tenants can reuse existing Wi-Fi APs and Ethernet switch ports.
- 5. **Fully-Managed or Partially-Managed:** Most services include partially or fully managed support, so enterprises don't have to handle provisioning, patching, upgrades, or other maintenance tasks. This applies to NaaS as well.

While these attributes are generally agreed upon by most NaaS vendors (as well as MSPs and enterprise customers), there is ongoing debate between upstart NaaS providers and incumbents about the true definition of NaaS.

CAMPUS NAAS REQUIREMENTS – FOUNDATIONAL AND EXPANDED

Table Stakes	Tables Stakes++ or Options
 Consumption Pricing	 All-inclusive Pricing (upgrades incl.)
 Low/No CapEx	 Zero CapEx
 Short-Term Commit	 Outcome-based SLAs (w/ penalties)
 Quick Provisioning	 Proactive Monitoring
 Fully/Partially Managed	 Fully Managed

 **AvidThink**

avidthink.com

What's in a Name: Half-NaaS versus Full-NaaS?

Upstart NaaS players accuse incumbent vendors of marketing pseudo-NaaS or half-NaaS, criticizing them for merely wrapping a financial model around legacy product-based sales. Some established vendors either can't or don't offer NaaS directly to their customers, instead relying on MSP partners to deliver NaaS using vendor products. These upstarts argue that such half-hearted attempts do not meet the critical criteria of a true or full NaaS offering. In addition to the essential as-a-service attributes mentioned earlier, upstarts contend that the following capabilities are necessary to qualify as full-NaaS:

- **All-Inclusive Pricing Model:** Covering hardware, software, maintenance, upgrades, and management. Pricing based on capacity or usage metrics. Some NaaS providers roll up internet connectivity as well.
- **Zero Upfront Capital Expenditure:** Not consistent across all upstarts — some ask for repayment of installation costs.
- **Outcome-Based SLAs:** With financial penalties for missed response times or uptime violations. Automatic periodic hardware upgrades to maintain performance SLAs.
- **Proactive Monitoring:** Experienced staff in network operations centers (NOCs) that monitor and mitigate any issues observed in customer network. Including preemptive hardware replacement to mitigate potential network issues.
- **Full Management Included:** Network engineering staff at NaaS providers that handle the complete lifecycle management of customer networks, from planning and design, site survey, installation, updating and upgrading, to maintenance, monitoring, and troubleshooting.

It's too early to determine if the full complement of additional NaaS requirements are necessary to adequately service most of the enterprise market; enterprises are just beginning to respond to the early waves of Campus NaaS providers. And the NaaS upstarts are not uniform in meeting all the additional criteria. Some upstarts lean on MSP partners for assistance, but their software stacks incorporate greater intelligence and automation, reducing the OpEx burden on their partners.

Regardless of its evolution, Campus NaaS is set to replace self-managed campus networks and will undoubtedly impact MSP or system integrator-managed networks. We anticipate that future managed services will move up the stack to focus on policy, complex management tasks, and security, rather than mundane and low-value tasks that will be codified and standardized by NaaS vendors.

Differences Between NaaS and Other as-a-Service Models

One last observation we'll make about NaaS versus other as-a-service models is that SaaS, IaaS, and PaaS are hosted in centralized data centers as pools of computing resources managed by cloud providers and accessible from any location on the global internet. After the initial data center build-out, provisioning services do not involve physical or mechanical labor. Virtual networking services that ride on top of existing physical networks can be managed in a similar fashion.

However, Campus NaaS involves deploying exclusive physical assets on customer premises. Wireless access points and switches must be shipped and activated for campus networks, even if zero-touch cloud-based software is utilized. There is inherent friction in NaaS offerings that require establishing a new network at a new location—especially one owned and controlled by enterprise customers.

Upstart NaaS players accuse incumbent vendors of marketing pseudo-NaaS or half-NaaS, criticizing them for merely wrapping a financial model around legacy product-based sales. Some established vendors either can't or don't offer NaaS directly to their customers, instead relying on MSP partners to deliver NaaS using their products.

Major Networking Vendors and NaaS

Many leading campus networking vendors today employ NaaS messaging and positioning in their literature. Some have used the "as-a-service" messaging for the last few years, but in its early forms, NaaS referred more to financing assistance than a complete NaaS offering.

The NaaS movements among large vendors are facilitated by their shift to cloud-based management. For example, Cisco's recent move to a Meraki-led cloud management overhaul for its Catalyst product family illustrates this trend. Infrastructure vendors like HPE, with its GreenLake initiative, are well-positioned to adopt Campus NaaS. While Dell offers its APEX as-a-service and Lenovo has TruScale, neither is a major player in campus networks.

Here's a quick overview of select major networking vendors and their expansion into Campus NaaS. Some well-known Wi-Fi/switching vendors, including Arista Networks, Cambium Networks, Huawei, and Ubiquiti, are not covered as they have limited or no NaaS offerings today.

- **Cisco Meraki:** Cisco's cloud-based Meraki portfolio offers a simplified, cloud-managed networking solution for wired and wireless infrastructure. Meraki provides network visibility, control, and automation across its hardware. Cisco primarily approaches NaaS through MSP partners, who leverage Meraki hardware and cloud-based platforms, combined with their services and financing assistance, to provide NaaS to enterprise customers. Many major MSPs (and managed service units at CSPs) offer all-in-one subscription pricing with one to three-year terms that combine fully managed design, installation, management, and monitoring services with the hardware.
- **HPE Aruba:** HPE Aruba is the largest incumbent networking vendor with a pure NaaS play at this point. Its strong cloud-based management of APs and switches is integrated into its broader HPE GreenLake initiatives. Aruba directly offers NaaS to its enterprise customers and enables its MSP partners to do the same. Aruba provides a monthly subscription model without requiring MSPs or enterprise customers to take ownership or lease the equipment. As one of the top three campus Wi-Fi solution providers, Aruba's embrace of NaaS is noteworthy.
- **Juniper Mist:** Juniper, which will soon integrate with HPE, acquired Mist Systems in 2019, bringing advanced AI capabilities through its Marvis platform to its cloud-based Wi-Fi solution. Juniper has been integrating its switching and routing portfolio with Mist's cloud and AI capabilities, providing a comprehensive NaaS offering. Juniper has promoted its NaaS solutions since 2022, supported by Juniper Financing Services (JFS), offering flexible financing options with one-, three-, and five-year terms and the option for JFS to hold the title. Management options include DIY through VARs or Juniper's managed services partners.
- **RUCKUS Networks:** RUCKUS, part of CommScope, markets its NaaS as a flexible set of offerings under the RUCKUS One converged platform. This platform allows customers to choose their level of managed services and offers flexibility in purchasing and financing. A unique feature of RUCKUS is its integration of private cellular (including CBRS) and IoT management under RUCKUS One, enabling enterprise NaaS customers to manage Wi-Fi, Ethernet switches, and private 5G through a unified console.
- **Extreme Networks:** Extreme Networks offers a unified management platform for wired, wireless, and SD-WAN products, available in the cloud or on-premises. Extreme markets its Network-Infrastructure-as-a-Service (NaaS) as an all-in-one subscription with hardware, software, and support, while retaining title (eliminating accounting overhead). Installation, design, and support can be purchased as professional services, and ongoing management must be obtained through Extreme's managed services partners.
- **Alcatel-Lucent Enterprise:** ALE, the enterprise division of Alcatel-Lucent owned by China Huaxin Post and Telecom Technologies, offers its OmniSwitch and OmniAccess product lines under the NaaS by ALE umbrella. ALE is committed to the "as-a-service" model across its product lines in communication, collaboration, and networking. ALE's offering provides flexibility regarding equipment purchase versus NaaS subscription, allowing for the addition or removal of services as needed.

With HPE's impending acquisition of Juniper, and if it continues pushing NaaS under its GreenLake program, the combined entity would be a significant force in the Campus NaaS market. HPE Aruba, combined with Juniper Mist's Marvis AI capabilities, zero-trust, and SD-WAN assets, could form an Enterprise NaaS platform that extends from campus switching to a converged suite of networking and security offerings for remote, branch, mobile, and campus IT.

Meanwhile, other incumbent players will likely continue to enhance their platforms by adding AI-powered operational capabilities to reduce OpEx and improve troubleshooting and reliability. We anticipate further integration of security features into campus networking platforms as enterprises seek fine-grained access control and better visibility over IT assets. Even as these established vendors incrementally evolve their offerings, a groundswell of new startups is entering the NaaS market.

Exploring the NaaS Upstarts

Several new players are emerging in the NaaS market, each with a unique approach and value proposition. Some have significant financial backing and leadership by networking veterans. Here's a look at five prominent NaaS upstarts.

Overview of NaaS Upstarts

Company	Founded	#Paying Customers	# Pilots	# Employees	ARR Growth (YoY)	Funds Raised
Join	2017	100-150	Not disclosed	50	300%	\$28M
Meter	2015	200-250	Not disclosed	80-100	300%	\$85M
Nile	2018	100-150	10-50	220+	300%	\$300M
Ramen Networks	2022	10-50	10-50	30+	250%	\$12M
Shasta Cloud	2022	Not disclosed	Not disclosed	Not Disclosed	Not disclosed	Not disclosed

Join



- **Target Verticals:** F1000 Corporate (High Tech, Biotech/Life Sciences, Financial Services, Energy, Media, Professional Services, Automotive/Transportation), Mid-market Enterprise (500-2000 employees)
- **Geographic Regions:** North America (US, Canada), Europe (early), Japan (Joint venture)
- **Pricing Model:** Subscription-based pricing that integrates software, hardware, and services into a unified package priced on a per-user OR per-space basis
- **Sales Model:** Direct to Enterprise, Direct to building owners and their tenants, Indirect Channel (Strategic Partners, MSP and referral partners, evolving to partner fulfillment)
- **Differentiators:** Pioneering Network-as-a-Service Offering—early leader in cloudifying LAN in 2018 with scalable, reliable, automated network; Fully-integrated End-to-End Solution—holistic approach with hardware, software, monitoring, and AI management, delivered through predictable subscription pricing; AI-Driven Network Operations Center (NOC)—proactive detection and resolution of network and security issues using AI and network data.

Meter



- **Target Verticals:** Education, Manufacturing, Robotics, Logistics, Hospitality, Technology, Retail, Professional Services
- **Geographic Regions:** North America, EMEA coming soon
- **Pricing Model:** Priced per sq ft
- **Sales Model:** Direct, Value-Added Resellers (VARs), Managed Service Providers (MSPs), Internet Service Providers (ISPs), Technical Service Distributors (TSDs), and consultants
- **Differentiators:** Fully integrated stack - develops its own hardware, network operating system, and cloud management allowing it to provide the best user experience with the highest performance and reliability in a cost-effective offering; claims first and earliest NaaS player - committed to full NaaS, not repackaged product with financing or MSP-wrapped product; co-managed platform allows offloading to Meter's services team or use of cloud-based management tools.

Nile



- **Target Verticals:** Carpeted enterprise, manufacturing/logistics, higher education, retail/warehousing
- **Geographic Regions:** North America, UK, EU, Japan, Saudi Arabia
- **Pricing Model:** 1/3/5 year all-inclusive contracts, billed monthly or annually on a per-building basis, either per square foot or per user
- **Sales Model:** Traditional channel partners, MSPs, and service providers
- **Differentiators:** Cloud-native software architecture with closed-loop automation powered by AI; high-performance wired and wireless with guaranteed coverage, capacity, and availability commitment; built-in zero trust campus security with per-device isolation.

Ramen Networks



- **Target Verticals:** Uncarpeted enterprise including logistics/supply chain, manufacturing and higher-ed. Mid-sized enterprises (\$100M to \$10B in revenues)
- **Geographic Regions:** United States, with Canada and Mexico planned in 2025
- **Pricing Model:** Based on area covered and SLA requirements. Contract 3-5 years. SLA commitments are resolved with additional equipment if needed. Ramen or the partner owns the infrastructure by default, but some customers prefer to own the hardware.
- **Sales Model:** 100% channel model and fulfill contracts through channel partners but participate directly in customer lead generation.
- **Differentiators:** Designs and deploys a solution leveraging LTE/5G and Wi-Fi using its own custom solution stack, including intelligent edge appliances for access gateways and video and IoT sensor processing services from third parties; includes hardware and software adaptors to connect any device and enterprise software application, and automated configuration and monitoring to reduce security risks; focus on solution stacks for video analytics (safety, sports, retail) using wireless cameras.

Shasta Cloud



- **Target Verticals:** Mid-market, MDU, hospitality, retail, education
- **Geographic Regions:** North America
- **Pricing Model:** All-inclusive subscription (HW, SW, Cloud Service, Support & HW refresh), \$x / AP or Switch / Month, 3 & 5-year payment options also available, Transparent pricing, no deal registration, no minimal order quantity for partners
- **Sales Model:** Exclusively indirect via MSPs
- **Differentiators:** Purpose-built system for MSPs—developed to support MSP processes and tools; Unlock enterprise white box platforms —diverse HW platform choice at factory direct pricing, single solution touchpoint; Developing unique copilot for MSPs to scale their workforce.

Common among all these upstarts is the positioning of incumbents as not offering true NaaS. They view true NaaS as subscription-based, SLA-backed with penalties for non-compliance, outcome-driven, all-in-one fully-managed (or co-managed if desired) network and security services, with the flexibility to add and remove components. Additionally, the vendor should upgrade and swap equipment as needed to maintain SLAs.

Each upstart has its own distinct positioning (which may converge over time):

- **Join** leverages its experience working with property owners and its joint venture in Japan, scaling to thousands of workers in dense office buildings, and integrating with workplace management systems to increase its appeal.
- **Meter** touts its fully integrated proprietary stack (own hardware, firmware, operating system, and cloud management) and a rich set of services, including ISP WAN, SD-WAN, firewall, and DNS security from Cloudflare. It also promotes its hardware buyback option, aiding customers in disposing of their existing equipment sustainably.
- **Nile** focuses on its AIOps capabilities, integrated zero-trust security, and custom-built stack, with the advantage of having John Chambers and Pankaj Patel as spokespersons, which helps open many enterprise doors.
- **Ramen Networks** concentrates on uncarpeted enterprise customers, offering a unified Wi-Fi and private 5G solution wrapped in an as-a-service model.
- **Shasta Cloud** uses white box hardware and open-source software (OpenWiFi and OpenLAN Switching) to enter the market quickly, investing in ease of management, MSP enablement, and tools for streamlined deployment.

Examining the three upstarts with over 100 customers reveals different origin stories and slightly different DNAs, but common among them is their networking experience and passion to remake enterprise networking.

Nile (Nile Global, Inc) is led by CEO Pankaj Patel, a seasoned ex-Cisco networking veteran (former EVP and Chief Development Office), and John Chambers (former CEO and Chairman of Cisco), who is a founder, board member, and investor. With \$300M raised and a large team of seasoned executives and engineers, Nile has set its sights on re-inventing campus networking and security, writing their software from scratch, and touting their fully integrated stack, along with advanced telemetry and AIOps capabilities. All eyes are on the all-star team as they seek to make a dent in the market against their former employer.

Meter, Inc., which has been around the longest (almost ten years), was founded by two brothers, Anil and Sunil Varanasi, who studied networking in college. Subsequently, they were convinced they could re-invent how internet infrastructure for enterprises was built, sold, and managed. Along the way, they convinced a who's who of Silicon Valley of their vision, garnering \$85M in funding to date from the likes of Sequoia Capital (which funded Cisco, Meraki, and other networking and security giants), Diane Greene (founder, former CEO of VMware), Sam Altman (OpenAI, Y Combinator), Patrick & John Collison and Lachy Groom (Stripe), John Bicket & Sanjit Biswas (Meraki co-founders), and Tishman Speyer (real estate conglomerate). With the longest time-in-market and the most significant number of paying customers, Meter is pushing hard to bring its NaaS vision to its North American customers, with European expansion in their sights.

Join (Join Digital, Inc.) was founded by Silicon Valley-based serial entrepreneurs Karl May and Dan Malek. Karl led the team that introduced the first broadband cable modem, connecting hundreds of millions of people to the internet, and Dan helped turn Linux into a real-time operating system. At Join, their vision is to write their own software, migrate network functions off appliances and make campus and branch networking a cloud service. During the pandemic, Join added advanced network and workplace analytics to create a more holistic solution. Join is leveraging its relationships with the owners of the largest commercial office assets — Boston Properties, Invesco, Oxford, Spear Street and a joint venture in Japan with Obayashi — in their go-to-market and address enterprise clients of these real estate giants.

Opportunities for NaaS Vendors

Looking ahead, the evolution of campus networking towards a true-as-a-service model will involve several key milestones reflecting technological advances, changes in institutional needs, and shifts in how IT services are consumed. Here are some anticipated milestones in this evolution:



1. **AI-Powered Service Automation and Orchestration:** While there are economies of scale in outsourcing network design, installation, and management to a specialized NaaS network operations team, there is always room for further OpEx reduction. AI/ML (including GenAI) and automation promise dynamic resource allocation, improved network performance, and reduced vendor operational overhead, making the network more responsive to customers' changing needs. This should translate to lower costs for enterprise customers, better margins for NaaS players, and an enhanced end-user experience.



2. **Adoption of Predictive Analytics:** Utilizing machine learning and predictive analytics to monitor network health and predict future needs will be a significant milestone. Vendors already have early versions, but there is much more potential. This capability allows vendor staff to proactively manage customers' network resources, anticipate problems, and optimize performance without customer intervention.



3. **Further Integration of Network Security:** With the rise in data breaches and cyber threats, enhancing security will be crucial. Advancements in AI-driven threat detection and response, encryption, and zero-trust (micro-segmentation) architectures will be essential to protect sensitive data and assets.



4. **Expansion into WAN Services:** Campus infrastructure currently includes campus gateway devices (routers, firewalls, and other security appliances). With the ongoing convergence of security and networking, we expect more NaaS players to incorporate SD-WAN (multi-link and 4G LTE/5G backhaul for resiliency) and SASE capabilities—SWG, ZTNA, and FWaaS.



5. **Integration of IoT and Smart Campus Solutions, Expansion into Private 5G:** As IoT devices are increasingly deployed for security systems, environmental monitoring, and more, integrating these technologies into NaaS offerings will be crucial. Whether cameras, sensors, and other ancillary devices become standard in NaaS offerings remains to be seen. Aligned with IoT and IIoT support for verticals like manufacturing, logistics, and retail, customer demand for private 5G and 4G LTE options is expected in environments where Wi-Fi performs poorly.



6. **Deployment of Wi-Fi 7:** The rollout of Wi-Fi 7 technologies will be a natural next step for all Wi-Fi vendors, including Campus NaaS vendors. Wi-Fi 7 offers faster speeds, reduced latency, and higher density, supporting a better user experience for wireless devices across campus. NaaS vendors will need to conduct ROI calculations to determine which customers should be upgraded and in what order, potentially driving tweaks to SLAs and contracts to clarify what triggers equipment upgrades.



7. **Customization and User-Centric Services:** As NaaS evolves, vendors will likely expand customized and user-centric services. This includes personalized access and security profiles, application-specific networking, and user-friendly self-service portals for managing network services and troubleshooting connectivity issues. We've seen vendors like Cisco make acquisitions to improve end-to-end visibility (ThousandEyes, SamKnows, Accedian), and there will be pressure on other incumbents and NaaS upstarts to match these capabilities.

Barriers to NaaS Adoption

Adopting Campus NaaS can offer numerous benefits to companies, such as offloaded network management, predictable spending, and increased focus on core capabilities. However, enterprises have expressed several concerns about NaaS, including:

1. **Dependency on Service Providers, Fear of Vendor Lock-In:** Adopting a managed NaaS solution means relying heavily on external providers for critical network operations. This dependency can raise concerns about service quality, response times for troubleshooting and repairs, and the provider's ability to meet specific campus needs.
2. **Security and Privacy Concerns:** Handing over the network infrastructure to a third party can raise security and privacy concerns, especially in environments handling sensitive research data and personal information. Ensuring that the provider meets stringent security standards and compliance requirements is crucial. In some organizations, security standards may dictate the use of specific vendors (who are not the NaaS vendor), making it complex to integrate both NaaS and the security platform.



- 3. Cultural Resistance:** Internal IT staff and other stakeholders accustomed to traditional network management approaches can resist adopting a NaaS model. Concerns about job security or shifts in job roles can also lead to resistance. Some NaaS players emphasize a co-managed approach in their sales process to allay these fears. Others target business owners or building owners who already outsource IT functions and simply swapping a NaaS vendor for an existing service provider.
- 4. Overhead of Integration and Compatibility with Existing Systems:** Integrating NaaS solutions with existing IT infrastructure, including legacy systems, can be complex. This integration must be seamless to avoid disruptions in network services and ensure that all parts of the campus network communicate effectively. In large organizations with a diverse array of IT technologies, getting NaaS solutions to interact and integrate with these assets might prove expensive and time-consuming for both the customer and the NaaS vendor.
- 5. Service Level Agreements (SLAs) Ambiguity:** Negotiating SLAs that align with company needs is vital. Many companies are unfamiliar with NaaS and worry that the SLAs don't cover all critical performance aspects, such as uptime guarantees, performance metrics, and support response times.
- 6. Technical Limitations:** Upstart NaaS solutions may have technical limitations compared to mature products. These limitations could restrict an institution's ability to implement specific technologies or customize the network as extensively as necessary. Enterprise customers need to closely monitor vendor roadmaps to understand when key capabilities will be added.



Recommendations for Enterprise IT Teams

Campus NaaS is a compelling response by networking vendors to enterprise demand for a network (and security) solution offered as a service. A growing number of customers have adopted Campus NaaS, whether from large incumbent networking vendors or upstarts. For small and mid-sized organizations and branch locations of large enterprises, Campus NaaS can be a cost- and time-saving approach to installing and upgrading campus connectivity without substantial capital expenses, tying up internal IT teams, or hiring consultants. Given the current state of the market, we recommend that enterprise IT teams interested in NaaS:

- **Talk to Other NaaS Customers:** Seek out NaaS customers in similar markets and of comparable size. There are sufficient NaaS deployments today among early adopters to conduct appropriate diligence.
- **Determine Desired Level of Control and Visibility:** Some NaaS vendors prefer to fully manage customer infrastructure, while others offer co-management options. Others require engaging their MSP partner to obtain a full NaaS solution.
- **Validate the OpEx Solution:** Ensure the NaaS vendor offers a true OpEx solution (if desired) and understand the contractual commitment (1, 3, or 5 years). Clarify what happens to equipment at the end of the term and the nature of equipment ownership.
- **Negotiate SLAs:** Determine the level and nature of SLA required and negotiate with the vendor on pricing. Most NaaS offerings are flexible on SLAs, and penalties have not yet been standardized. Understand when and how hardware upgrades will occur and how network underperformance is monitored, detected, and resolved.
- **Pilot Testing:** For large organizations, evaluate Campus NaaS options for remote campuses and branch locations and run trials before expanding coverage to central campuses. For smaller organizations, run a pilot to gain experience.

Conclusion

The NaaS market for enterprise campus networks is in its early stages but holds significant promise for organizations seeking to simplify network management, improve agility, and reduce costs. With established vendors and innovative startups entering the space, the NaaS landscape is evolving rapidly. Most enterprise software has migrated to an “as-a-service” business model, and a large portion of enterprise computing and storage has followed. Networking is likely to migrate in the same direction, and this transition could be accelerated due to the prior transitions in computing and storage.

While challenges remain, including concerns about vendor dependence, IT job security, data security, privacy, and compliance, the potential benefits of NaaS are compelling. As technology advances and best practices emerge, NaaS is poised to become a mainstream approach for campus networking, enabling enterprises to focus on their core business while ensuring a secure, reliable, and high-performing network experience for their employees. By 2030, a majority of middle, small, and perhaps even large enterprises will be consuming some flavor of NaaS along with converged network security. We'll be carefully tracking the evolution of this space. Reach out to us at research@avidthink.com if you have further questions.



AvidThink, LLC
1900 Camden Ave
San Jose, California 95124 USA
avidthink.com

©2024 AvidThink LLC. All Rights Reserved.
This material may not be copied, reproduced, or modified in whole or in part for any purpose except with express written permission from an authorized representative of AvidThink LLC. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgment of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.