EBOOK

connect
what matters most

If You Aren't Modernizing Your Network, You Can't Digitally Transform

5 key principles to ensure today's networks meet tomorrow's challenges

aruba
a Hewlett Packard Enterprise company

Table of Contents

When networks can’t keep up

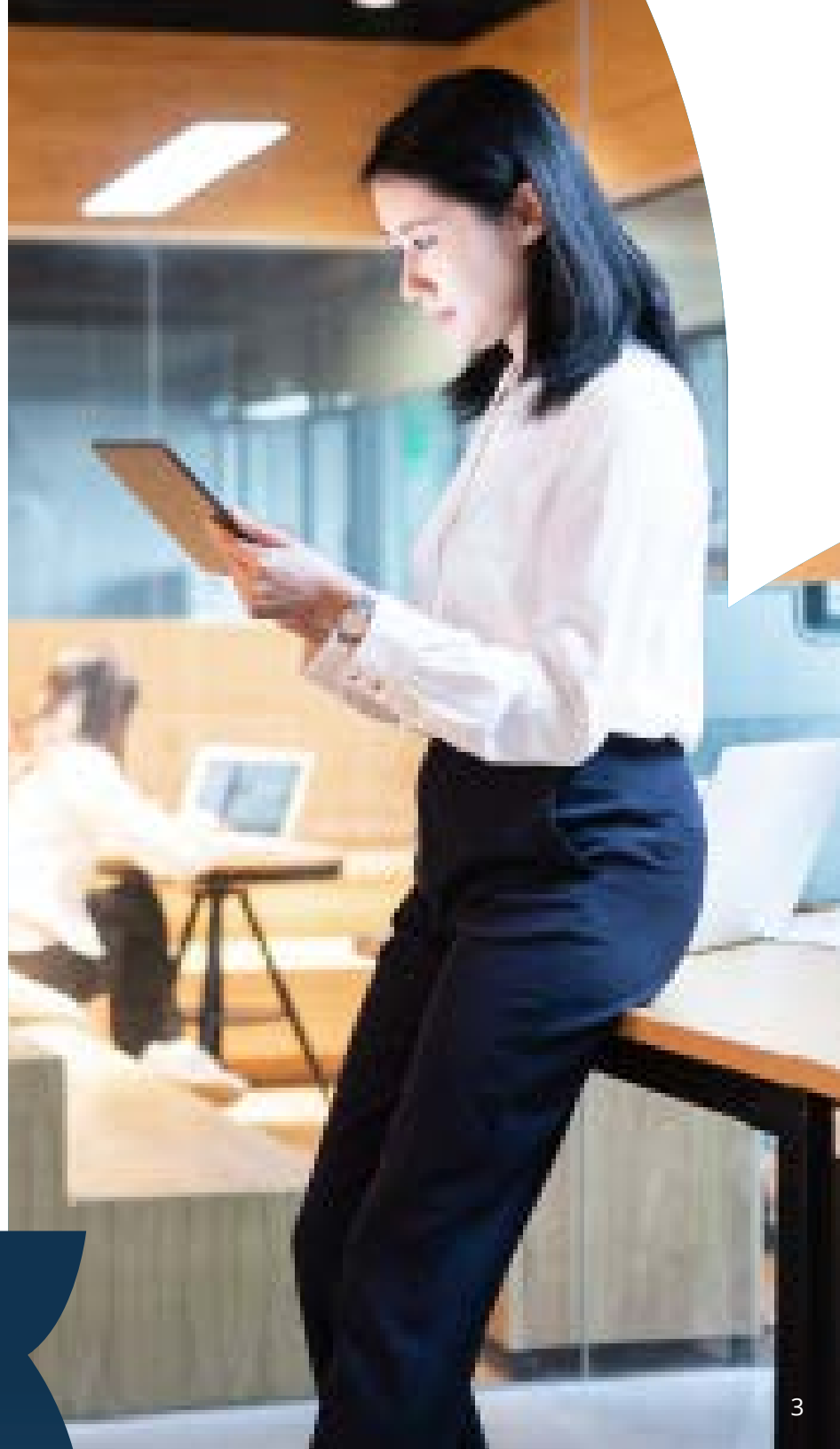
The network acts like a central nervous system for today’s digital business. Yet for most organizations, it’s not up to the task of directing the growing volume and diversity of data connecting people and things, whether physical or virtual. A suboptimal network can lead to scenarios where:

- Remote workers are second class citizens
- New business models are stalled
- Employees and customers have subpar experiences
- Massive amounts of IT resources are wasted on archaic, manual processes
- Dangerous security gaps create vulnerabilities

Network modernization equips enterprises to address architecture, operations and security related challenges as they begin or accelerate digital transformation efforts. Modernization is necessary to support new business models, changing workforce trends, and demands for improved employee and customer experiences. Here’s what network modernization delivers:

- Faster deployment of new network solutions, cut from days and weeks to minutes
- A stronger security foundation based on Zero Trust and SASE
- Unlimited network scalability
- Access to new consumption models that relieve budget and staff constraints
- More consistent user experiences from the edge to the cloud

This eBook examines the core issues driving the need for network modernization. It addresses five key functional principles and offers practical suggestions for how to make sure your network meets the needs of your business.



Coping with increasing complexity

The networks of yesterday resembled rigid, multi-tier hierarchies and were (and still are) difficult and expensive to reconfigure and manage. Today, organizations expect networks to efficiently and seamlessly support hyper-distributed edge environments characterized by an increasingly remote workforce, the rapid growth of IoT-connected devices, and a continuing need to provide secure connectivity to applications, services, and data hosted in the cloud and data centers.

Yet, adapting yesterday's networks to this new environment creates multiple levels of operational challenge:

- **Scaling networks** with potentially hundreds of thousands of users and devices, across a wide variety of locations and connection types, is manual and requires custom configurations. Performance inevitably suffers and SLA's become increasingly hard to meet.
- **Scarce IT staffing resources** and the overwhelmingly manual processes required to set up and configure networks means that too much time and energy is wasted on basic moves, adds, and deletes–leaving few resources to focus on strategic business initiatives.
- Without a strong network security foundation, **protection gaps** are more likely. The network and security teams need to work together to defend against cyberattacks while implementing industry-recognized security frameworks such as Zero Trust and Secure Access Service Edge (SASE). New network architectures often require a **wholesale replacement of current infrastructure.** This results in premature obsolescence and vendor lock-in.
- Traditional purchase and service delivery models make it **difficult to rapidly acquire, manage, and finance new network solutions.**

"Traditional networks made up of multiple product lines, tools, and interfaces are rigid and complex to manage. Updates and changes to the network can be risky, requiring significant product expertise and time. Network issues of any kind—configuration, provisioning, troubleshooting, problem resolution, security, optimization—restrict business agility and worker productivity." **Enterprise Software Group**

You may get the money, but will you deliver results?

Business is recognizing the value of shoring up technology assets. The 2022 State of the CIO report found that 59% of IT decision makers expect increased budgets, and only 10% expect a decrease.

The top 3 reasons tech budgets are increasing:

- 57%: Need for security improvements
- 48%: Need to upgrade outdated infrastructure
- 48%: Investment in new skills/talent

5 ways to modernize your network now

The challenge for network decision makers lies in building a network for the future, when expectations are likely to vary greatly from what we know today. That's why network modernization is not a destination, but a continuous process. As such, it is critical to take advantage of cloud-native services – whether consumed in the cloud or on-premises—that provide the agility to adjust to changing business requirements as they occur.

A modern network must work equally well and integrate across a remote workers, branch office, campus, data center, and cloud while providing a new architectural approach that is edge-centric, cloud-enabled, and data-driven, offering organizations simplicity, speed, and security packaged into flexible consumption models.

Network modernization can look like a big project, but organizations can manage their modernization activities and investments and prioritize their efforts based on five key foundational principles aimed at gaining performance, automation, security, and agility with ease and efficiency.

Principle #1:
Connectivity and scale

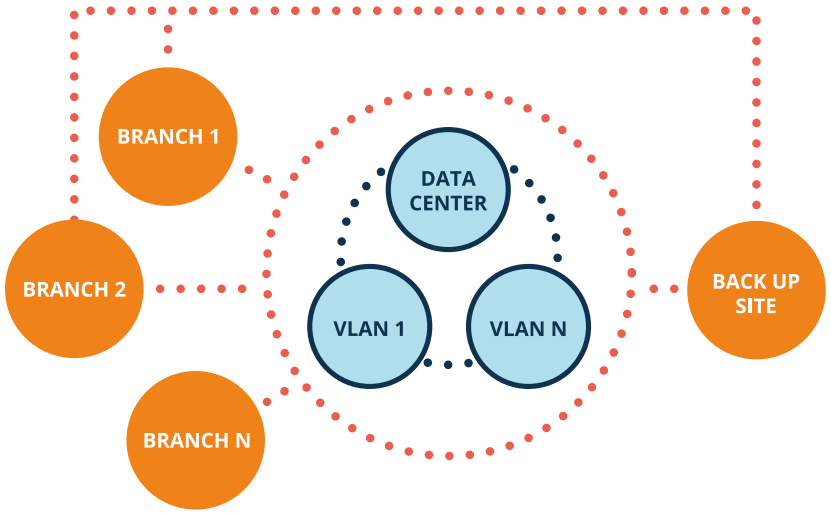
With remote work, IoT, and new business models creating hyper-distributed environments, networks based on traditional VLAN architectures will struggle to accommodate potentially hundreds of thousands of users and devices, across a wide variety of locations and connection types.

That is why new protocols and architectures are essential for scale and connectivity. For example, EVPN-VXLAN (Virtual Extensible LANs) enables businesses to connect geographically dispersed locations and isolated VLANs using layer 2 virtual bridging over a layer 3 network. The expanded address space of EVPN-VXLAN enables the creation of up to 16 million separate networks. This overcomes a key limitation of VLANs, which can create a maximum of 4094 separate networks and dramatically expands the ability to create fine-grained traffic segmentation policies.

In addition, stitching together VLANs across a widely distributed environment across a widely distributed environment is manual and requires a significant amount of custom switch and gateway configuration. This typically means that the traffic travels on inefficient routes and there is constant "care and feeding" of the network segments. Once the network is operating properly, daily management, troubleshooting, and optimization are equally manual and inefficient and will cause IT to fall short of SLAs and user expectations.

In addition, the modern network provides a cloud-native single point of control to give administrators visibility and ease of management across wireless LANs (WLANs), LANs, and SD-WANs deployed in campus, branch, remote worker, data center, and cloud locations.

Layer 2 Overlay (e.g. EVPN/VXLAN)



Layer 2 network overlays such as EVPN/VXLAN create a "superhighway" for more efficient traffic flows and comprehensive security enforcement

What you can do now:

- Deliver a secure network quickly and cost-effectively using cloud-based services. Choose a cloud-native solution that delivers the agility and timeliness of the cloud whether you consume it in the cloud or on-premises. Start with branch locations, a new facility, or a project like a campus refresh so the IT team can experience how easy it is to power up wireless access points (APs), switches, and gateway infrastructure while centrally configuring the network and security policies through a single point of visibility and control.
- Introduce network overlays such as EVPN/VXLAN alongside existing infrastructure to learn how to adapt these protocols to current and future environments. The key is to select an approach that will coexist with what is in place today and not require a wholesale "rip and replace" of your current investment. For future growth, make sure that the same management and architecture works across wired, wireless, and WAN connections.
- Modernize your WAN solutions with SD-WAN. With greater flexibility, efficiencies, and cost savings, internet broadband is the preferred wide-area access method given the prevalence of cloud-based workloads and the economics of internet connectivity. Look for an SD-WAN solution that works with the selected network overlay fabric, and has integrated support for security frameworks such as SASE.

Principle #2:
AI-powered automation

The scale of modern networks is already exceeding human capabilities to monitor, troubleshoot, and optimize the organization's connectivity assets. Talent is increasingly scarce, so throwing more people at the problem is not only undesirable, but also not easy to do.

Organizations need to massively reduce the time and resources required to plan, deploy, manage, and optimize highly distributed networks. Automation is the only answer, and it's going to take artificial intelligence (AI)-powered automation of operations (AIOps) to make it successful.

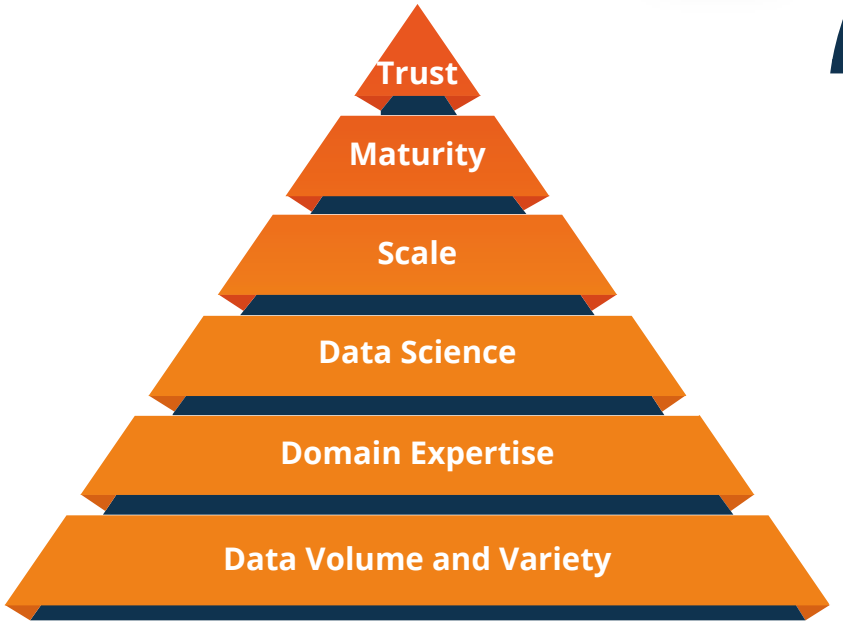
AIOps is a human-assistive technology that enables administrators to work on higher-value tasks by automating repetitive tasks such as configuration management, RF optimization, and troubleshooting. AI-powered solutions automatically and securely collect and analyze data from various sources to anticipate issues, automate specific tasks under operator control, and optimize overall network performance.

AIOps improves the efficiency and effectiveness of network operations from planning to Day Zero deployment and Day-N ongoing management. Once a network is set up, AIOps provides the ability to automatically surface and diagnose network-impacting issues by using dynamic, per-site baselines that are continuously tuned as conditions change, without requiring manual setup or adjustment of service-level thresholds. Built-in anomaly detection highlights the severity and effect of issues as they occur, helping IT pinpoint root causes and proper remediation steps with very high accuracy.

AIOps can help solve troubleshooting issues up to 90% faster, while reducing trouble tickets by 50% simply by seeing issues before the user does.

What you can do now:

- The use of AIOps is a culture shift that may leave some staff wondering if it will eliminate their jobs. It won't. Work with your team to introduce the ideal of using AI to reduce the time and effort spent on mundane tasks to free them to work on more interesting and strategic projects.
- Start small to test how AI solutions work in your environment. AI conclusions should have a "fail safe" button where the network admin must agree to a change before it is implemented and a "change back to the previous state" button for recommendations that did not work out. AI is very good in a lot of situations, but it isn't perfect.
- Learn how to spot "AI washing" by vendors who will make bold claims without the ability to deliver. The first question to ask is: "How much data feeds your AI models and where does it come from?" The right answer starts with a customer base of 100,000 or more. Then consider domain expertise, proven track record, and applicability across all sizes of organizations. Anything less means the AI can't be trusted.



Beware of "AI washing." Five criteria to determine if you can trust AI for network operations

Principle #3: Security

Cyber security strategies must accommodate an ever-changing, diverse set of users and devices connecting to the network. Managing legacy networks with manual processes is not only inefficient and impractical, but it also creates visibility gaps and potential security vulnerabilities. It is prone to human error as well. Plus, latency causes unacceptable delays in responding to potential data breaches.

Relief for IT and networking managers can come from the increasing integration of networking and security functions. Zero Trust and SASE frameworks provide a blueprint for a secure network foundation that uses identity-based access control built into the network to protect the organization.

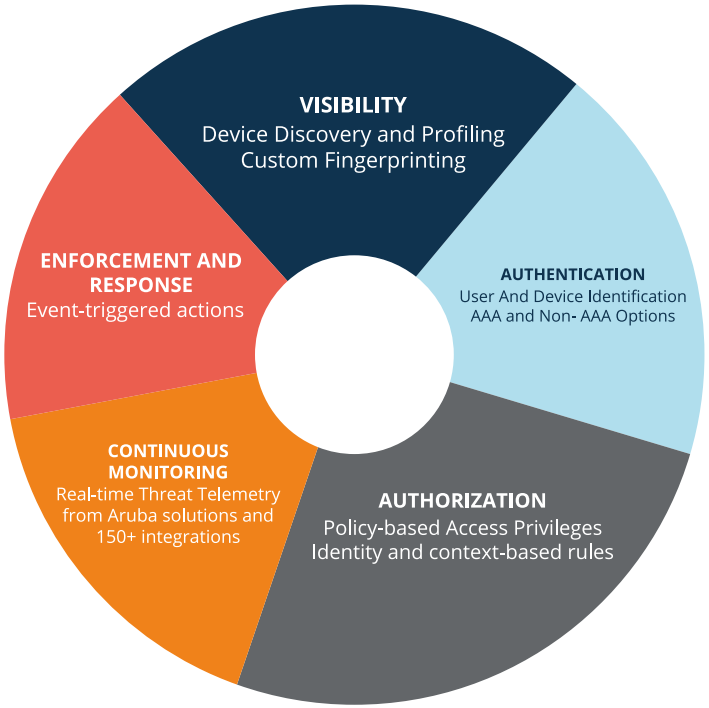
Today, IT must assume that no user, device, or network segment is inherently trustworthy. Zero Trust architectures ensure that all devices and users trying to access the network are identified and authenticated, before providing the least amount of access required through a predefined security policy.

A foundational principle of Zero Trust and SASE is that access permissions are independent of the method of connection. Once on the network, validated devices and users must be continuously monitored so that there is full visibility into who and what is on the network and what activities are taking place.

There are five key functions required to implement identity-based access control in support of Zero Trust and SASE:

1. Have no blind spots. Use AI-based techniques to see IoT devices that have connected to the network outside the purview of network and security teams.
2. Authenticate all users and devices using a combination of 802.1x, multi-factor techniques, device fingerprints, etc.
3. Authorize access permissions based on the user and device identity, the role that IT has assigned them, and the access privileges associated with that role.
4. Enforce and monitor. Segment traffic based on access policies and continuously monitor endpoints in conjunction with the broader security ecosystem to spot changes in security state that could imply a compromise.
5. Respond to attacks by dynamically changing roles and access privileges. This can range from bandwidth throttling to quarantine to outright blocking. Together, Zero Trust and SASE can ensure that the same access controls applied to campus or branch networks also extend to the home or remote worker across wired, wireless, and WAN connections.

Together, Zero Trust and SASE can ensure that the same access controls applied to campus or branch networks also extend to the home or remote worker across wired, wireless, and WAN connections.



Zero Trust and SASE depend on identity-based access control enforced by the network

What you can do now:

- If the network team and security team are not already working together, look for ways they can collaborate and use the same tools to configure and manage both the configuration and traffic policies as well as security policies. The network management system should provide the UX/UI tools to facilitate this integration.
- Insist that Zero Trust and SASE are built into and integrated with network solutions rather than being bolted on after the fact. Those solutions should provide for consistent policies and controls that enable the network to discover, identify, and authenticate devices and users attempting to gain access; enforce configuration compliance and role-based access control; and segment network traffic based on permissions incorporated into access policy.
- The network and the security ecosystem must work together so organizations can optimize their investments with best-of-breed solutions. For example, as SASE-based solutions become more prevalent as workloads move to the cloud, networking functions such as SD-WAN must seamlessly integrate with a wide range of cloud-delivered security services for the best overall networking and security outcome.

Zero Trust and SASE on the rise

• 57% of respondents say their organizations have either deployed or will deploy Zero Trust.

• 49% of respondents say their organizations have either deployed or will deploy SASE architectures. – **Ponemon Institute survey**

What's the point of Zero Trust?

"Endpoint prevention and protection stops malicious activity; endpoint detection and response finds what slips by; micro segmentation prevents its spread; and the crack security operations center uses security automation to remediate." — **Forrester**

Principle #4:
Flexibility and agility

Rapidly changing business objectives require a network that can quickly – and automatically—adjust to new or changing conditions.

Unfortunately, many organizations today are constrained by a patchwork of disparate solutions to manage WAN, wired, and wireless networks for remote workers and campus, branch, and data center locations. This siloed approach requires the use of multiple, domain-specific network management tools. Fragmentation of this magnitude creates operational friction that is far too manual and inefficient.

The agility of a continuously modernizing network takes several forms. First, cloud-native network solutions can provide a single point of visibility and control across wired, wireless, and WAN, along with a consistent workflow and user interface that breaks down domain silos. By their nature, cloud-native solutions will deliver a continuous stream of updates and new functionality that keeps an organization at the leading edge.

But cloud-native does not necessarily mean deployed in the cloud. While that is an increasingly common option, many organizations choose to remain on-premises with key IT solutions for a variety of security and control reasons. So, an important principle of agility is to be able to deploy the same functionality in either scenario.

Another principle of network agility is the ability to introduce new architectures and topologies without making current investments obsolete. As noted above, new security paradigms or the use of network overlay fabrics should not require a wholesale "rip and replace" of current infrastructure to take advantage of their increased functionality and performance. This allows for a migration path that incorporates new solutions at a pace that is comfortable for the organization.

Vendor lock-in is another threat to agility. Often, seemingly standards-based products will deviate from widely-adopted protocols to ensure that once they are implemented, the customer has no choice but to stay with that solution. This creates a "walled garden" that is extremely difficult to interoperate with third-party solutions. in contrast, modern networks are open and easily accommodate best-of-breed integrations that complement and enhance the overall solution.

Finally, agility comes from the tools that the networking team can leverage to make changes quickly and confidently. Are workflows driven by graphical user interfaces that reflect business intent without requiring knowledge of the underlying infrastructure? In other words, can they leave the world of command line interface? When deploying wireless access points, are they self-locating or does the staff need to consult blueprints and manually map each device? When physical changes occur, do the device maps automatically adjust? Network management solutions that offer this kind of "force multiplier" significantly increase organizational efficiency.

Whether in the cloud or on-premises, cloud-native network services deliver the agility that modern networks require

What you can do now:

- If you haven't begun your cloud journey for network management and identity-based access control, pick a project or part of your network that would benefit from centralized cloud control and visibility. A great place to start is with remote work environments where Zero Touch Provisioning, AI-powered oversight, and consistently applied security policies create the same experience at home as in the office. If you are already using cloud-native network management, make sure it can scale to your needs and deliver the functionality you require. Many cloud solutions started out as small business tools and are trying to "grow up" to be enterprise-class without the architectural underpinnings to work in larger environments.
- Insist on cloud-native services that can be deployed either in the cloud or on-premises to integrate setup, configuration, and management in a single "pane of glass" for visibility and control. You should be able to replace manual configuration of static VLANs and access control lists with business-intent policies that define network topologies, traffic flows, and proper access privileges for employees, guests, contractors, and other user groups.
- Keep a close eye on licensing terms. In some cases, licenses are written to lock customers into current equipment or to force them to upgrade before they are ready.

Principle #5:
Employ as a service

Many organizations face difficult, often seemingly insurmountable, challenges in rapidly acquiring, implementing, managing, and financing new network solutions. Long-term CAPEX and depreciation constraints, scarce staff resources, and skills shortages can create long product life cycles and an inability to shift quickly to meet changing business dynamics. Today, many if not most organizations would prefer to focus on business outcomes rather than planning for end-of-life acquisition processes.

Alternative consumption and deployment models, including self-delivered or managed- services, flexible financing, and new technologies provide more options, more agility, and reduced time to market than traditional acquisition and deployment models.

Just as organizations overcame compute and storage limitations through adoption of public and hybrid cloud infrastructure, they can now take advantage of network-as-a-service (NaaS) consumption models. This approach delivers new network solutions quickly, while optimizing budget resources with easier scalability – flexing either up or down.

NaaS provides the flexibility to consume enterprise network infrastructure in a way that enables organizations to keep pace with technology innovation, meet rapidly changing business needs, and optimize network performance and user experiences through a choice of a CapEX or cloud-like subscription model, even when the infrastructure is located on-premises.

In one model, NaaS can alleviate the burden of long-term network planning and budgeting by delivering all hardware, software, and services in a single monthly subscription, with no upfront capital investments required. Organizations get access to the latest and greatest technology, while easing the burden on their IT staff and allowing them to address high-priority business challenges and deliver new network solutions quickly while optimizing budget resources.

New survey says NaaS has arrived. 1/3 have already deployed with another 25% committing in the next year

- 60% say long-term planning cycles now down to 2 years
- #1 catalyst: more rapid deployment of new technologies
- 41% opting for OpEx vs. CapEx
- 82% consider sustainability benefits important

Source: 2022 IDC NaaS Global Survey Sponsored by Aruba

What you can do now:

- Evaluate the potential that a flexible financing and subscription approach can offer your organization and whether your vendor has the resources to support a significant as-a-service model.
- Ask your vendors if they provide NaaS options for replacing aging, in-place solutions and whether they have standard service offerings, or is every deal a custom scope of work? Mature NaaS vendors understand how customers want to consume services and can streamline the ordering and delivery process.
- Determine if your organization needs, and whether your vendor or partner can provide, NaaS options to offload day-to-day network monitoring, administration, and operations to free up internal resources for more value-added activities.

Outsource as much as you want

"NaaS models allow enterprises to outsource the planning, deployment, day-to-day operational management, upgrades, monitoring and troubleshooting of an enterprise network, as well as decommissioning and end-of-life support of equipment. Through that process, organizations get access to the latest technology offered by the NaaS vendor, including new hardware components and software." — **IDC**

Why modernizing networks is worth it

Network modernization isn't simply an exercise in updating current infrastructure to keep up with the next generation of technology. It's an essential, ongoing process to create an agile network foundation, which advances the organization's ability to implement digital transformation initiatives quickly by taking advantage of new approaches to architecture, security, management, and delivery.

But a modern network is not some future, hard-to-reach state. With the suggestions noted above, there are pressing business issues today that can best be addressed by embarking on a modern network foundation:

- Extending the on-campus experience to small offices, home offices, and mobile users with ease
- Developing location-aware services to provide seamless experiences, both indoors and outdoors
- Leveraging the data generated by the rapid growth in IoT devices
- Relieving the skills shortage by automating network operations
- Providing efficient, consistent, and secure access to cloud-based applications from wherever users are located
- Automating configuration and management of complex network and security processes with workflows tied to business intent
- Reducing the time and resources required to plan and implement change with new consumption and deployment models
- Leveraging AI-powered analytics to reduce the time to troubleshoot issues, significantly cut down the number of trouble tickets, and take advantage of community best practices to optimize network operations
- Empowering customers, employees, and guests with new digital experiences

How Aruba can help

Aruba is enabling network modernization, wherever you are in your edge-to-cloud journey.

Aruba has repeatedly been recognized by third-party analysts as a leader in network connectivity options such as: Wi-Fi, switching, and SD-WAN. As a Hewlett Packard Enterprise company with hundreds of thousands of customers from small/medium businesses to global enterprises worldwide, Aruba provides a secure, AI-powered edge services platform that spans all networked environments.

At the forefront of innovation since its start in 2002, Aruba offers network modernization across each of the five principles with Aruba ESP (Edge Services Platform).

With Aruba ESP, Aruba takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments. Aruba ESP delivers faster everything—user connections, IoT onboarding, scaling of secure locations, issue resolution, and operational insights—on a single architecture.

As the management and orchestration console for Aruba ESP, Aruba Central simplifies and improves IT operations with a cloud-native, single point of visibility and control for WLAN, LAN, and SD-WAN. This includes AI-powered insights, workflow automation, and robust security that enables IT to manage and optimize campus, branch, remote, data center, and IoT networks from a single dashboard.

And given the role of the network in building Zero Trust and SASE frameworks, Aruba Central provides organizations with full visibility, control, and enforcement of identity-based access control and traffic segmentation across the entire infrastructure.

No matter where you are in your digital transformation journey, Aruba can guide you firmly on the path to network modernization–now and into the future.

To find out more, go to:

www.arubanetworks.com/connectwhatmatters

ebook_aruba_network-modernization_031522

aruba

a Hewlett Packard Enterprise company