aruba

a Hewlett Packard Enterprise company

EBOOK

5 Reasons to Make the Shift to Cloud-Managed Networking

5 Reasons to Make the Shift to Secure, Cloud-Managed Networking with Aruba Central

Take the Next Step in Modernization with Cloud-Managed Networks

Cloud has proven advantages for the enterprise. Modernizing IT with cloud apps, compute, and storage has delivered greater collaboration, rapid innovation, and cost efficiency across all business departments.

Networking is the next area for cloud adoption. The shift is well timed, as traditional networks are overwhelmingly complex to manage, and often negate the benefits cloud computing was supposed to deliver.

50% of new network deployments will be managed via cloud-based platforms by 2022[1]

42% of organizations plan to or have already adopted SD-WAN to improve IT agility and delivery of cloud apps[2]

30% of enterprises will adopt AI-enabled tools to augment traditional monitoring approaches by 2023, up from 2% today[3]

[1.] IDC, "Five Key Enterprise Networking Trends to Watch in 2020," April 2020
[2.] Ibid
[3.] Gartner, "Use AIOps for a Data-Driven Approach to Improve Insights from IT Operations Monitoring Tools," May 2020

1 Improve Network Agility to Keep Pace with Digital Innovation

Digital transformation has accelerated. Businesses are looking to unlock competitive advantages by optimizing supply chains, creating compelling experiences for customers and employees, or even ushering in entirely new business models. Nearly 60% of business interactions are digital today, up from 36% in 2019[1].

Networks will continue to play a pivotal role in delivering applications, data, and the resulting digital experiences to end users. Unfortunately, legacy, manually-driven networks are holding businesses back.

Implementing necessary network changes on a device-by-device basis is time-consuming, tedious, and costly. Manual operations of this nature require costly truck rolls to dispatch skilled IT personnel from site-to-site and often result in delays, cost overruns, and operator errors.

[1]*Source: McKinsey & Company*

Manual network operations increase risk of issues

26%
of network problems are caused by human error

Source: "EMA, Network Management Megatrends 2020"

Conversely, cloud-managed networks make it far easier to deploy new services or entirely new sites. Capabilities such as zero touch provisioning enable IT to preconfigure devices such as access points, switches and gateways. Upon arriving onsite, devices are plugged in, powered up, and automatically receive their configurations and policies from the cloud. Network connectivity is up and running in mere minutes.
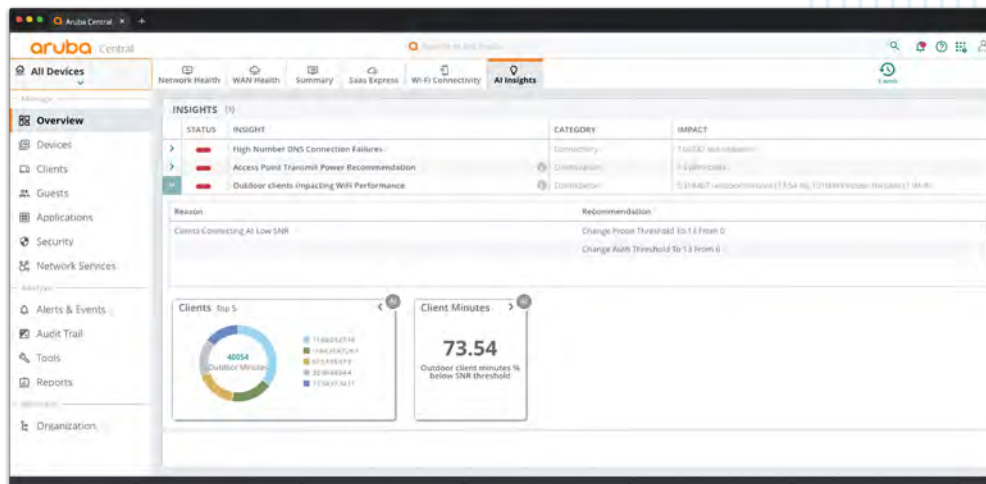
Similar efficiency can be gained during change windows. From a cloud-based management console, IT can stage configuration changes just once, instantly validate those updates conform to network policies and are error-free, and then instantly push the new settings to every applicable device across the network.

Cloud-driven workflows such as these enable significant cost- and time-savings by reducing errors and rework, as well as costs and delays associated with onsite IT visits.

75% of processes that result in error can be avoided with automation.

Automated changes also **cost less than 2%** of what they do when completed manually.

Source: Gartner

| 5

2 Use AIOps to Free Up IT for Strategic Work

Manually configuring the network isn't the only time-consuming activity. Nearly 60% of IT's time is spent addressing network issues[1].

AIOps helps IT spot issues before they become actual problems. In this case, the use of AI and machine learning make sense of massive amounts of metadata stored in the cloud, translating raw information into clear insights and recommended actions.

Dynamic Baselines

A key AIOps feature is the ability to dynamically baseline network behavior over time, automatically accounting for changing conditions such as seasonal traffic patterns. This way, IT doesn't chase false positives, as alert fatigue can also be a resource drain.

Dynamic baselines are also beneficial because it's time-consuming for IT to manually set and maintain static service-level agreements (SLAs) for every site. With real-time insights into network behavior, IT can instantly see and respond to actual issues.

[1]*Source: EMA, Network Management Megatrends 2020*

5 Benefits of AIOps and Network Automation

1. Optimize the user experience

2. Accelerate network service delivery

3. Increase network reliability

4. Ensure consistent network configuration

5. Resolve issues faster

Anomaly Detection

Through the use of anomaly detection, IT can automatically identify and begin addressing issues – oftentimes before users notice there's a problem. Better yet, with the right level of AI-driven insights, the probable root cause is pinpointed, so IT knows precisely what to fix, and how to fix it. Issues are also categorized based on severity, helping IT prioritize changes and improvement efforts based on business impact.

Peer or Site Comparisons

Lastly, cloud-managed networks can make use of anonymized peer comparisons from a common data lake. Here, insights are gathered and presented from customers with similar site or network characteristics, so IT can proactively make configuration changes that may ultimately yield performance or capacity improvements over existing infrastructure.

How Can AI Optimize Networks?

A retailer was experiencing sluggish Wi-Fi performance at its stores. But IT lacked the data or benchmarks to accurately diagnose and fix the problem.

With **AIOps**, the problem was identified and validated. As returning customers walked past the store, their devices were attempting to reconnect to the in-store Wi-Fi. A recommended configuration change eliminated 98% of this unwanted "passerby" traffic, helping improve performance for legitimate users.

The result: 25% more wireless capacity without any new hardware.

3 Monitor and Improve the User Experience from Anywhere

People have high expectations for an excellent user experience when accessing applications and other digital services over corporate networks. However, assessing and improving application performance is increasingly difficult, as most IT monitoring tools fail to account for the end user's actual experience.

As a result, one-third (33%) of network or application issues are reported by end users[1], meaning IT is often in reactive mode when addressing business-impacting problems. This also assumes IT is onsite or has the right levels of remote access to troubleshoot the issue in the first place.

A cloud-managed networking solution can help by empowering IT to monitor user, device, and application performance from anywhere. Solutions that offer client-side monitoring that mimic user behavior provide further insights, helping IT assess and validate the impact network changes have on applications and the employees or customers attempting to connect to them.

[1]*Source: EMA, Network Management Megatrends 2020*

4 Support Teleworkers, Minus the IT Overhead

COVID-19 witnessed an unprecedented number of teleworkers. Work-from-home is here to stay, as many employees will continue to work remotely at least part-time.

In the hybrid workplace, employees access business applications over a variety of networks – both inside and outside of IT's control. Due in part to variable network conditions, 70% of businesses have teleworkers who experience IT performance issues at least multiple times a week.

Cloud-managed networking helps deliver in-office experiences, no matter where employees work. Such solutions can extend secure connectivity into employees' homes, either via remote access points or a VPN service. Both options should be easy for any employee to install, and should provide reliable access to apps and data – all while maintaining a secure connection.

IT gets full visibility and troubleshooting support via the cloud to address and resolve issues. This way, IT can reduce costs tied to addressing support tickets and the exponential impact of avoiding work stoppages.

TELEWORK IS HERE TO STAY

70% **of US and EU companies will shift to hybrid work after COVID-19.**

Source: Forrester, May 2021

5 Stronger Security for BYOD and IoT

Supporting teleworkers may be the new normal, but security will always be a concern when employees access corporate resources outside the traditional IT perimeter. Meanwhile, back at offices, businesses are deploying more IoT devices, which are fundamentally untrustworthy, and a lack of visibility creates greater risk.

Cloud-based networking can help IT extend security policies and approved levels of network access wherever employees go – onsite, on the road, or at home. Policy-based automation replaces static concepts like VLANs or ACLs, and capabilities such as intrusion detection and prevention block incoming threats coming from SaaS applications delivered over the Internet.

To close IoT visibility gaps, consider solutions that offer AI-based device profiling that continuously fingerprint all devices on the network. By tracking device usage and behavior, IT can ensure proper policies are being enforced.

IoT CREATES GREATER RISK

80% **of IT orgs have found IoT devices on the network they did not install or secure.**

Source: Gartner, February 2021

The End Result:
Higher Efficiency, Lower TCO

Cloud-managed networking is a powerful way to deliver operational excellence for IT infrastructure and operations teams. Here are four ways organizations can realize better ROI and reduce networking TCO:

TCO Savings

- Reduced server costs
  (no heating, cooling, or maintenance)
- Reduced truck rolls
  (fewer onsite visits, lower travel costs)
- Reduced labor costs
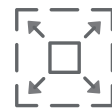 (far less errors and rework)

Improve IT Productivity

- Unified management
  (no manual correlation or moving from tool to tool)
- AI-driven operations
  (simplifies troubleshooting and updates)
- Automated software updates
  (limits maintenance windows)

Increase IT Agility

- Easily deploy networking from campus to remote offices
- Easy to turn on new capabilities
- No server or sizing changes

Enhance Resiliency

- Higher scale
  (microservices architecture and web-scale design)
- Higher availability
  (hosted by cloud provider data centers globally)

aruba

a Hewlett Packard
Enterprise company

At Aruba, Secure Networking Is Our Mission

Simplify how you provision, configure, and maintain networks by orchestrating all operations from a cloud-native dashboard. Aruba Central is your single point of visibility and control that spans the entire network – from branch to data center, wired and wireless LAN to WAN.

Learn more at www.arubanetworks.com/central