Technical brief

Simplify architecture for secure hybrid work, better user experience

Evolve your network and data center to improve performance, availability, and security

Innovation is moving faster than ever. Digital is at the heart of the customer experience. Employees work from anywhere. Data drives business decisions and process automation, with data volumes growing exponentially. Generative AI (GenAI) promises new possibilities for innovation. Cloud-first strategies have increased business agility, but many apps remain in private data centers. Users, apps, and data must be accessible anywhere and protected anywhere.

IT leaders are at the forefront of turning digital transformation ambitions into reality. At the same time, IT teams are challenged to manage and secure their hyperdistributed infrastructure. To accelerate business agility, organizations must modernize—and simplify—their IT architecture from edge to cloud. Simplification can deliver better network performance, availability, and security, all with greater operational efficiency.

Enable business agility with a simpler architecture

Businesses want cloud-like agility, whether their applications are in the cloud or a private data center. Businesses need to be nimble to deliver exceptional digital experiences to customers, enable employees to work securely from anywhere, and drive innovation through data-intensive analytics and GenAI apps.

Advancing key innovation initiatives while ensuring that employees, contractors, customers, and business partners, have fast, secure access to critical digital services, applications, and data across a complex hybrid, multicloud infrastructure is challenging—and getting harder. Managing and securing today's networks demands time-intensive manual work by multiple teams, leading to overwhelming efforts to deliver the necessary application availability, zero trust security, and operational efficiency.

The benefits of simplifying architecture and enhancing security

Simplifying your network architecture, including in the data center, can deliver the agility you need to advance key business initiatives.

When you modernize and evolve your data center network, you can enhance application and network performance, extend zero trust security to protect sensitive workloads and data, and reduce the cost of IT operations. Modernizing doesn't have to mean a rip and replace either, but rather, it should be a nondisruptive evolution to meet the application and workload demands.

Simplifying architecture also improves network availability and performance. A modern architecture leverages next-generation switches that can deliver orders of magnitude performance and scaling over traditional switches. Real-time network telemetry and AI-powered operations can dynamically optimize network performance and availability, resulting in improved business outcomes and operational efficiencies.

Don't let complexity stand in your way

Most data center networks were not architected for today's data-driven businesses, hybrid multicloud world, and work from anywhere approaches. Most organizations use a stateless data center fabric architecture that limits performance and scale, preventing IT from delivering network services with cloud-like agility. Critical network and security functions are effectively bolted on, creating unnecessary complexity. Creating and managing network services to support application service delivery requires a heavy lift from multiple technology teams.

You may recognize the signals that the time is now to modernize your data center architecture. Signals to watch out for include:

— Inconsistent application performance for software-as-a-service (SaaS), cloud-native, and legacy applications

— The need for more specialized appliances to handle firewall, load balancing, encryption, network address translation, and other essential functions, but add latency and increase architectural complexity

— Rising data privacy and compliance risks due to sophisticated threats hiding in data center workloads or bypassing perimeter defenses

— Fragile network and security infrastructure that is risky to update or replace

— IT teams need different tools to manage campus, data center, and security domains, restricting visibility and limiting control

— An IT team overwhelmed by day-to-day operations, leaving scant time or energy for innovation

Realizing a simpler, more secure architecture

A simpler, more secure data center architecture is within reach. Rather than modernizing in the future, you can start now. You can increase network performance, enhance security, and drive cost efficiency. When getting started, consider this checklist:

— **Does your data center fabric provide integrated security services?**

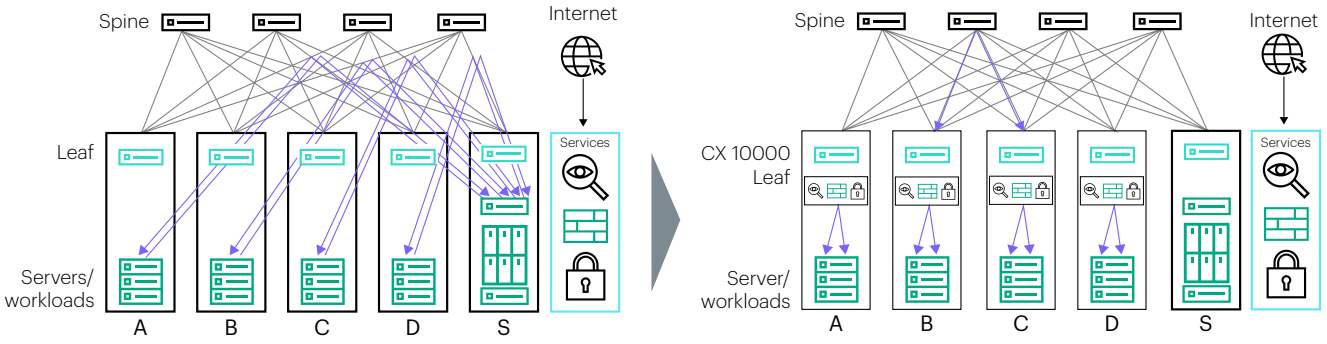
The modern approach to data center fabrics enables you to downsize those racks of firewalls, load balancing, and other specialized appliances that are necessary with today's stateless data center fabrics. Next-generation data center switches leverage a distributed services architecture, using purpose-built data processing units (DPUs) to perform services like network address translation, encryption, and distributed denial of service (DDoS) mitigation. You can deploy security and network services at the switch port level, improving performance, bringing security closer to your workloads, and reducing the overall data center footprint.

— **Can you automate network provisioning and operations?**

Smart orchestration tools can take the struggle out of manual, siloed network configuration and management. Instead, you can orchestrate a group of switches as a single network fabric to speed service provisioning and simplify day-to-day operations. With increased visibility and control over the fabric, you can solve connectivity and performance issues before the business is impacted. Cloud-based management tools can extend that visibility and control across your environment from edge to cloud, so you can ensure that users have fast, secure access to private apps, SaaS, and internet resources, whenever and wherever they are.

— **Can you extend zero trust to the data center?**

Modern data center switches actively secure the network to protect your business from threats that have evaded perimeter defenses. You can extend zero trust microsegmentation, firewall, and encryption closer to your most sensitive security workloads to reduce risk of business disruption from data breaches, ransomware, and denial-of-service (DoS) attacks.



Legacy DC network design
» Traffic having to hairpin to L4–7 services leaf/rack
» Unable to scale to match east-west traffic
» High and cost complexity (appliance sprawl, licensing)

Next-generation, secure network fabric design
+ Embed network and security services at each leaf port
+ Improve app performance
+ Retire legacy appliances and agents
+ Automate security policy and provisioning

Figure 1. Addressing legacy data center network challenges with a next-generation, secure network fabric

Improve network availability and performance with HPE Aruba Networking

To simplify data center architecture and enhance security, take these steps:

Step 1: Improve network availability, performance, and security—at your own pace

HPE Aruba Networking has created a fourth-generation fabric architecture that leverages DPUs and application services that provide enhanced security, performance, and intelligence. The HPE Aruba Networking CX 10000 Distributed Services Switch with AMD Pensando™ simplifies data center architecture and enhances security—without disrupting the architecture or software configuration.

Organizations can deploy HPE Aruba Networking CX 10000 Switches as top-of-rack, leaf, or access switches to enable stateful services like firewalls, network address translation, encryption, and DDoS mitigation. Security functions are delivered in line and at scale and closer to where applications and workloads are processed. There's no need to offload essential network functions to specialized appliances, which simplifies the architecture and reduces application latency. HPE Aruba Networking CX 10000 Switches provide 800G of distributed stateful firewall, zero trust segmentation, and advanced telemetry for rapid troubleshooting.

Step 2: Simplify network management and operations

HPE Aruba Networking simplifies and accelerates network provisioning and day-to-day operations. IT teams can orchestrate a discrete set of switches as a single fabric to simplify operations and troubleshooting, simplifying configuration and unifying security policies and distributed firewalls across the fabric and even across multiple data center locations. Real-time telemetry provides the foundation for AIOps and automation.

IT teams can use HPE Aruba Networking Central, a cloud-based management solution, for AI-powered insights, intuitive visualization, and smart workflow automation for universal visibility and control across campus, branch, and data center networks.

Organizations can also tap into HPE consulting services for expert advice and implementation help to take their data center transformation to the next level. HPE Aruba Networking can help you simplify your architecture from edge to cloud so you can deliver exceptional user experiences, support secure hybrid work, and meet the demands of data-intensive apps.

Learn more at

HPE Aruba Networking CX Switches

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

AMD is a trademark of Advanced Micro Devices, Inc. All third-party marks are property of their respective owners.

a50010490ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com