aruba
a Hewlett Packard Enterprise company

DICKER DATA

The (un)official operator's guide to next-gen networks

It's time for network transformation

Organizations embracing IoT, cloud, and other digital technologies can't move forward with networks rooted in the past. Legacy switching infrastructure, in particular, is oversubscribed, and the use of outdated network management tools increases the likelihood of errors, missed deadlines, and extra costs.

Bring your business into the future by enhancing your network with a modern switching infrastructure and a cloud-like management experience. Explore the following key components of a modern, next-gen network to begin your transformation journey.

Improve IT agility with a cloud-native operating system

Networks need to be as nimble, elastic, and resilient as other IT infrastructure. A modern operating system based on the following cloud-native principles provides the foundation for network operational efficiency.

Modularity

To improve process quality, every feature of the network operating system should operate independently, much like microservices-based applications. An operating system based on a publish-subscribe (pub-sub) model is key so that if one module needs to reference another, it subscribes to that module's information in the operating system's state database and reacts to changes as needed.

Resiliency

Modularity goes hand-in-hand with the second design principle: resiliency. Decoupling communication between software modules leads to better system performance and reliability. For instance, if a process fails, it should gracefully restart without disrupting the operations of other functions.

Programmability

Today's networks need to be programmable, without requiring developers or SDKs. Adequate REST API coverage and pre-built scripts or apps help IT operators easily integrate network infrastructure and state information with third-party platforms or tools, streamlining workflows across multiple IT systems.

Elasticity

A single network operating system should address any requirement from the access layer at the edge through the core and into the data center—without performance limitations or tradeoffs. With this level of elasticity and flexibility, the same OS can power a 1U switch in access wiring closets, as well as robust chassis switches in data centers.

A single operating model spanning from edge access to the data center

Traditional networks are hampered by disparate architectures and fragmented operations at each layer of the network, creating insurmountable complexity. Maintaining multiple operating systems is another issue, as costly subscriptions are often required to enable different software features.

Dramatically simplify network designs and ongoing operations with a **unified, end-to-end operating model** that offers the flexibility to deploy common hardware and software at each network layer. Leveraging a common operating system and management toolset can also promote tighter collaboration among traditionally siloed networking teams by sharing data and standardizing workflows.

Automation aligned to current and future operating models

Manual tasks are the bane of a network operator's existence. Pushing out changes device by device using CLI increases the likelihood of issues or outages due to human error. Such processes also inhibit networking teams from keeping up with evolving business requirements.

Automation is an integral component of next-gen networks. However, fully automated operations won't happen overnight. IT should embrace a combination of the following to support current and future operating models:

- **Turnkey automation** for common, large-scale configuration changes, which validates compliance with network policies as updates are rolled into production
- **Integration with DevOps tools** extends automation to network-related workflows, which is especially useful in environments that use orchestration engines like Ansible
- **Custom, event-driven automation** that enables the network to take corrective actions based on certain triggers or conditions, often without operator intervention

75% **OF MANUAL ERRORS CAN BE REDUCED BY NETWORK AUTOMATION**[1]

Simple, yet robust solution for always-on infrastructure

While ensuring high availability (HA) has been a longstanding network requirement, planning for HA involves complex tasks to address backup and failover processing—tasks that become even more time-consuming as networks grow.

Finding time to complete software upgrades is equally vexing. Upgrades are typically scheduled during periods of non-peak network usage, such as nights or weekends. In-service software upgrades (ISSU) are intended to shift maintenance to more reasonable times. But ISSU procedures are typically complicated, which increases the risk of errors and aborted upgrades.

70% OF NETWORK CONFIGURATION IS DONE MANUALLY[2]

A simple, yet robust solution that ensures high availability of critical network infrastructure should provide:

- **Resiliency at the software level:** A function that fails can restart—quickly and automatically—without disrupting the performance of other software modules. As a result, one failed process won't bring down an entire switch, nor have a cascading impact across other network devices.
- **Always-on availability at the hardware level:** Modular switches combined in an HA pair maintain independent control planes yet remain continuously synchronized. Such an architecture delivers on the promise of ISSU, without complexity or risk.

Distributed analytics to proactively isolate and resolve issues

IT operators continue to spend a majority of their time firefighting performance issues, due in part to highly reactive and time-consuming methods for monitoring and troubleshooting networks.

Approaches such as streaming telemetry to a central collector or using third-party monitoring tools limit the amount of data that's available, how quickly it's accessible, and how actionable it is—potentially leading to longer service disruptions.

Capturing and processing telemetry natively on each switch offers operators actionable insights into network-wide health, without delays or loss of information. With these **distributed analytics**, IT can detect application or network health problems in real time, rather than relying on complaints from end users.

Analytics tools that accelerate root cause analysis by predetermining many first- and second-order diagnostics are also a plus, freeing operators to focus on more pressing issues. Using these same insights, IT can analyze usage trends for capacity planning and predict or even avoid future issues.

39% OF PROBLEMS ARE DETECTED AND REPORTED BY END USERS[3]

aruba
a Hewlett Packard Enterprise company

DICKER DATA

Elevate the network operator experience

Networking leaders must prepare for the growing IT complexity that will stem from IoT, mobile, and cloud initiatives.

Analytics, automation, and always-on availability should be focal points of network modernization—helping IT operators rapidly investigate and fix problems, ensure network resiliency, and simplify common processes.

To learn more about delivering a next-gen operator experience, visit:

www.arubanetworks.com/switch-forward

Footnotes:

1. Gartner, "5 Network Cost Optimization Opportunities," June 2019.
2. Ibid.
3. Enterprise Management Associates, Network Management Megatrends 2018.