4 Ways to Modernize Your Campus Network for Digital Transformation

Table of Contents

Networks are expanding rapidly and relentlessly in response to changing user needs. Enterprises should modernize their approach to campus networks to support their digital transformation and provide a secure, always-on network that is automated yet simple to operate. Here's how you can make that a reality.

Organizations everywhere—from enterprises to hospitals and manufacturing plants—are accelerating use of mobile technologies to run their daily operations. And enterprise mobility is being redefined by the dramatic uptick in adoption of the Internet of Things (IoT) across a wide array of applications, environments and business processes.

This means your organization's wireless network is going through a transformation, as it needs to support more devices, "things" and applications and provide a good user experience. Business stakeholders require a modern network that delivers always-on connectivity for running mission-critical data and enhanced security as new vulnerabilities arise. Also, as networks scale and become more complex, network operations need to be simplified and include a high degree of automation.

Requirement No. 1: Always-on Connectivity

If a wireless network doesn't offer the reliability enterprises have come to expect from their wired networks, it obviates many of the intrinsic benefits of mobility in general and wireless networking specifically.

In an increasingly mobile-first business environment, always-on connectivity is a top wireless networking requirement, particularly for organizations that rely more and more on the network for mission-critical data such as voice and video. So, for instance, if a wireless LAN (WLAN) controller fails and a user is on a Skype business call, the network needs to remain up and running and the user's call should not be affected.

TechTarget | Custom Media

aruba
a Hewlett Packard Enterprise company

Also, upgrading the network operating system to the latest version usually requires scheduled maintenance time, which could affect workforce productivity in enterprises and manufacturing plants and be almost impossible in a healthcare environment with 24/7 operations. And as the security landscape changes and threats become more prevalent, new patches get released more often, requiring more frequent OS upgrades.

Given these factors, the modernized network must support always-on connectivity to support the business goals of the organization—without debate or exception.

Requirement No. 2: Automation

As networks scale, organizations can't solve problems with manual intervention anymore. They need to bring more automation to the network to deliver high performance in dense environments and ensure a good user experience. Automation also results in fewer errors than what occurs in most legacy networks. Organizations need a self-healing network to align with changes in the environment.

Automation is a must and should support features that dynamically adjust RF planning based on network changes due to a boost in the number of clients, for example, and automatically prioritize certain business-critical applications. Also, use of machine language engines instead of manual intervention is quickly becoming the preferred approach for many network management functions.

Requirement No. 3: Security

IoT is everywhere and changing everything. From smart lighting to Internet-connected equipment such as MRI machines and HVAC systems, operational technology (OT) is increasingly merging with information technology (IT) to increase the efficiency of conducting business. However, as the IoT and always-on mobile workforce expand, IT infrastructures are more exposed to attacks than ever before. Unlike laptops and mobile phones, IoT devices don't come with security software.

To accommodate today's modern network and provide security yet simplify management for IT and OT, organizations need a unified approach to security across both wired and wireless infrastructure. Having a single policy for all users, regardless of where or how they connect to the network, makes it far easier for network administrators to track policy and secure connectivity.

Requirement No. 4: Simplified operations

There is little debate about the increasing complexity of networks at all levels—endpoint devices, protocols, access methods, traffic monitoring and management, security and more.

To scale enterprise networks to meet the increasingly complex and demanding needs of users accessing applications, data and services from the network, organizations must have a centralized view of the entire network. Only through a single, comprehensive dashboard can enterprises manage everything from configurations and policy to capacity management.

An important element of simplified operations is ensuring a flexible approach to deployment models. For instance, more and more enterprises are moving toward virtualized environments, which gives them more compute power to do data analysis and automaton while providing ease of operation and simpler deployment.

What the ideal modern wireless network must deliver

Wireless technology has enjoyed significant breakthroughs recently, making wireless a viable solution for mission-critical enterprise workloads. Still, not every wireless network offers the same level of functionality and scalability, so it's important to look for certain features and capabilities when evaluating wireless network platforms to ensure high performance.

Those include:

- **A revamped, modernized network design** optimized for **always-on connectivity**, since the slightest interruption or downtime can impact productivity and user experience and lead to financial consequences.
- A platform that is **engineered for scalability and simple to operate, and provides a centralized view of the network**. This has become a core requirement as wireless networks handle more workloads, users and data.
- **Built-in intelligence and automation** to actively monitor, manage and act on network insights. This enables proactive identification of potential glitches that could affect anything from bandwidth availability to the number of security vulnerabilities.
- Multiple **deployment options**, such as the ability to stand up a virtual machine or an x86-based physical appliance, depending on an enterprise's environment and needs.
- **Policy consistency** across wired and wireless infrastructure.

Aruba WLAN with ArubaOS 8

Aruba, a Hewlett Packard Enterprise company, is a pioneer in the development of wireless networking and an acknowledged innovator in pushing the envelope for wireless network performance and availability. It has driven the move toward always-on networks with the release of **ArubaOS 8**, a wireless networking software platform designed for digital workplaces.

An important new element in ArubaOS 8 is **Mobility Master**, which allows customers to use a wide range of features built around centralized coordination and the ability to scale easily and seamlessly as demands spike across mobile devices and IoT systems. It can be deployed either as a virtual appliance or an x86-based hardware appliance.

Among the key ArubaOS 8 components required for a modernized network are:

- **Live Upgrade,** which eliminates the need for downtime during an operating system upgrade. Live Upgrade enables real-time upgrades with zero downtime and with no users impacted.
- **Seamless failover** in the unlikely event of a controller failure, enabled by clustering multiple controllers. User session information for voice, video and data is shared across controllers in the cluster, avoiding the single point of failure that often brings down older wireless networks.
- **Automated user and access point load balancing** using controller clustering, which contributes to an enhanced user experience, especially as the traffic load changes on the network.
- **RF optimization with AirMatch,** an automated tool that handles channel and power planning and channel width tuning as networks change in density and requirements. It uses a machine learning algorithm to automatically generate an optimal view of the entire wireless network.
- **MultiZone,** which allows IT and networking professionals to have multiple, separate secure networks but still use the same access point in the same physical location. This is very useful in malls or airports, where multiple networks are running.
- **Centralized Configuration,** providing a centralized view of the network to manage configurations more efficiently. This feature simplifies network configuration by enabling a certain part of the network to be grouped based on function or geo-location, such as a warehouse vs. a call center, and apply configuration for those access points at once.
- **Dynamic Segmentation,** which allows unified wired and wireless policy to be applied to mobile devices and IoT. It segments the network automatically based on device profiles and diverts traffic to the controller for further inspection and policy enforcement.

A Vertical View of the Always-On Network

With mobility making up a bigger part of the way employees and their virtual counterparts—contract workers, partners, suppliers and others connecting to the backbone network—do business, having an always-on network and ensuring a good user experience becomes the norm. This is true across all industries and vertical markets, from traditional brick-and-mortar establishments to businesses leading the way in digital transformation.

Take healthcare, for instance. As hospitals and clinics increasingly rely on mobility and IoT medical devices as well as personalized healthcare, mobile enterprise networks become the foundation for delivering a user experience that is always on and secure. And as the healthcare network scales, automation becomes key.

Higher education is another industry in which mobility is the pre-eminent form factor for a wide range of digital processes, from campus-wide education networks and social media to campus security, streaming media and cloud-enabled e-commerce. Millennials have grown up with mobility and wireless, and they demand always-on access to network resources and services in order to study, interact with others and enjoy their time on and off campus. They require seamless roaming, from when they leave their dorm rooms all the way to their classrooms.

Finally, so-called smart digital workplaces are on the rise. Such business environments are marked by a rich palette of devices, applications and data streams and layers of software. Together, this “connected fabric” is linked throughout organizations via mobile devices and wireless networks that deliver the sophisticated analytics and improved user experience necessary to drive greater productivity and enhance business value.

Smart digital workplaces are fast becoming the global standard for everything from space management, safety and security to technology tools that enable users to work and connect anywhere, at any time.

Conclusion

As networks grow in scale and complexity, organizations need to move quickly to modernize their networks to increase reliability, automation, manageability and security.

The newest generation of wireless technology from innovative suppliers like Aruba enables organizations to pioneer new applications and use cases and differentiate themselves from those that remain tethered to legacy infrastructure, which can be costly to maintain and complex to manage.

Organizations looking to achieve all the operational and economic benefits of a modern, secure network that is highly reliable with always-on connectivity and automation but simple to operate should consider architecting their wireless networks based on the latest version of ArubaOS from Aruba.

For more information on the Aruba WLAN and ArubaOS 8, please visit www.arubanetworks.com.