www.pipelinepub.com
Volume 20, Issue 4

Leveraging Cloud Native Principles and Automation for Next Generation WLANs

By: Suresh Katukam

Over the past 26 years Wi-Fi has proven itself to be the bedrock of today's Local Area Network (LAN). As a result, it also serves as the foundation upon which most of today's businesses function. That said, the ongoing "digital transformation" driving so many business decisions today is bringing massive changes to IT infrastructure as we know it. This is driven by the continued migration of enterprise data and applications to the cloud. With the vast majority of enterprises running mission-critical applications in a "cloud first" approach and consuming services like Zoom and Salesforce via a cloud-based subscription model, the question is not if, but when, this paradigm shift will impact the enterprise wireless LAN, a historically hardware-dependent network model that has proven itself resistant to change.

Why Apply Cloud Native Principles to the Wireless LAN?

Why seek to change a model that has proven itself so effective? The reason is that priorities have changed. Enterprises today are shifting focus to business outcomes rather than simply maintaining technology infrastructure. A CIO colleague explained, "I want my high-value people doing high-value work, not spending all their time keeping the lights on."

As it exists today, IT is forced to spend a significant portion of its operational resources "keeping the lights on." Consider the following aspects of today's network model:

- Many boxes of self-contained technology and monolithic software.
- Complex configurations baked into the hardware.
- Painful software upgrade cycles.
- Limited automation.
- Limited data collection.
- Separate AI models are required to generate insight.

Multiple decades of layered complexity eat into every budget, security, and performance compromise in developing the wireless LAN today. Today's CIOs don't care where APs are located or what version of 802.11 is running. They only care that the network is working as intended and that their teams are

working on building their business. If we are to free IT to focus on high-value projects that move the company forward, applying cloud native advantages to enterprise networks should be a priority.

What Does a Cloud Native Wireless LAN Look Like?

First and foremost, a cloud native wireless LAN is delivered via a cloud-based subscription model. IT has made it clear they prefer to consume their applications and services via this route. In the case of a wireless LAN, this service may be delivered by a channel partner, a traditional telco, or even a technology vendor. This includes zero upfront capital expense with no hardware to purchase. In fact, many legacy enterprise network vendors have recognized the advantages of this approach and have begun to offer rudimentary Network-as-a-Service (NaaS) offerings, but the simple truth is that the majority of these offerings amount to the same old hardware-centric model hidden behind a curtain of clunky services.

Second, and related to the cloud-based subscription model, a true cloud native wireless LAN eliminates the need for IT to manage the product lifecycle. That means not managing the transition between Wi-Fi 5 to Wi-Fi 6, 6E, or even 7. It means never having to cobble together switches, controllers, and five different kinds of Access Points (APs). The burden of maintaining this technology should fall on the entity delivering the cloud-based service. This frees IT to focus on the applications and services running on the network itself instead of having to spend time evaluating new hardware and figuring out how to integrate every new generation of wireless technology.

Third, a cloud native wireless LAN should incorporate zero-trust network security principles as part of its foundation. In short, security must be baked into the network from the beginning. There is little doubt that cybersecurity events represent an existential threat to businesses everywhere. Most hardware-centric, on-premises models are vulnerable to rogue APs, Evil Twin networks, and Man-in- the-Middle attacks that threaten enterprise data. By incorporating zero-trust network security principles, which were designed for the decentralized architecture of the cloud, a cloud native wireless LAN can ensure that any device that connects to the network is verified and monitored while connected.

Finally, a wireless LAN that incorporates cloud native principles should be able to deliver the same kind of guarantees that IT has come to expect from other cloud services. When a firm contracts with AWS to run critical applications, it has specific expectations and guarantees on uptime and reliability. IT needs to expect similar guarantees from a wireless LAN regarding coverage, capacity, and reliability.

What Technologies Are Involved in Delivering a Cloud Native Wireless LAN?

In order to build a next-generation wireless LAN based on cloud native principles, there are several common strategies and technologies that must be employed. Taken together, it should be safe to characterize the coming next-gen wireless LANs as AI networking. Industry analyst giant Gartner defines AI Networking in the following way: “AI networking delivers granular and specific actionable network insights. It can be a feature within a network vendor’s management platform, a stand-alone multi-vendor platform, or a part of an AIOps platform. It can also be delivered as part of a managed network service…[I]t offers recommendations to accelerate incident resolution and prevent outages and trouble tickets.”

First among these common strategies is standardized system design. The idea behind this approach is to eliminate the need to build unique architectures for each and every property that requires wireless

connectivity. Short of designing physical infrastructure to determine optimal coverage and performance, each cloud native wireless LAN should leverage the same APs and switching infrastructure governed by a decentralized management architecture. This is highly differentiated from today's wireless LAN model that requires IT to choose from five different kinds of APs, multiple switch models, and different controllers on a building-by-building basis.

Once a standard architecture is implemented, 24/7 network performance monitoring should be driven by sensor-based technology. Sensor-driven network performance monitoring, which includes both physical and virtual "bots" placed strategically throughout the network, enables proactive monitoring of the network and the applications running on it. Configured with the appropriate policies and deep instrumentation, the network itself will alert IT when an anomaly has been detected. This may be a performance issue, a security breach, or a critical outage in an important application. The point is that this job is performed by the wireless LAN rather than IT personnel. It also results in very rich and deep insights into the performance of the wireless LAN and the applications running on it.

These insights bring us to the next key to implementing a cloud native wireless LAN: AI-driven automation. This is a distinct capability from the current AIOps trend, which provides insights into Day 2 operational trends, but rarely does anything with these insights. AI automation provides productivity-saving functionality from Day 0 onward, dramatically reducing network operations overall. This means the network can actually identify and resolve minor network issues on its own.

This means that once the standardized network design and sensor-driven insights are in place, IT has the ability to fully automate the majority of network operations. This includes everything from the placement of APs to orchestrating software upgrades to identifying cabling issues using voltage sensors. For example, continuous RF optimization and capacity planning by the network will enable IT to add and subtract new users with ease. In fact, by employing cloud native principles, IT should be able to effectively do away with the traditional need for a Network Operations Center (NOCs), thus freeing its team to focus on higher-level priorities.

Making the Leap to the Next Generation Wireless LAN

Today's CIOs are just beginning this transition from traditional wireless architectures to more advanced cloud native principles. Much as businesses took time to acclimate themselves to running mission-critical applications in the cloud, CIOs used to running NOCs will need time to grasp the productivity, security, and reliability benefits of a wireless LAN based on this new architecture. There will undoubtedly be challenges to this transition, particularly from those who may feel their roles are threatened by the levels of automation involved. But these same "threats" occurred in the transition to the cloud, and skilled IT staff are still very much in demand. The roles will shift, but the need remains and will almost certainly even grow over time. And shift they will, as this transition, much as the shift to the cloud before it, is a certainty.