MARAVEDIS
Wireless Infrastructure Analysts

The Case for Cloud Wi-Fi

WHITE PAPER

Table of Contents

Executive Summary 2

1. Towards an Agile Cloud WLAN 3
   - 1.1 Evolution of IEEE 802.11 3
   - 1.2 Management, Control, and Data Planes 3
   - 1.3 Five Generations of WLAN Architecture 4
   - 1.4 One Size Cloud Does Not Fit All 6
   - 1.5 The importance of APIs 6
   - 1.6 Towards Open Standards 6

2. Drivers for moving Wi-Fi to the Cloud 7
   - 2.1 The Power of the Cloud 7
   - 2.2 Soon all wireless in the office? 8
   - 2.3 Benefits of Cloud-Managed Wi-Fi 8
   - 2.4 A comparison with on premise Wi-Fi 10
   - 2.5 Who should consider moving to Cloud Wi-Fi? 12

3. Fears and Myths about Cloud-Managed Wi-Fi 12

Considering Mojo 14

Conclusion 15

References 17

Executive Summary

Since Wi-Fi was first introduced in 1997 with the IEEE 802.11-1997 wireless standard, wireless networking has become the dominant wireless access technology in enterprises worldwide. Over the years, the architecture of wireless local area networks (WLANs) has evolved to keep pace with changing wireless needs and updated 802.11 standards and amendments. As WLAN has become more critical and reliable, the concept of All-wireless office is becoming a reality for many organizations.

WLAN architectures have spanned five generations: autonomous access points (APs), centralized controllers, hybrid controllers, cloud controllers, and distributed control with cloud management. As more and more organizations are driven to cloud-managed Wi-Fi, it is important to understand the drivers and iterations of the latest cloud-managed WLAN approaches.

This white paper discusses several drivers of cloud-managed Wi-Fi, including the evolution of the workplace towards more mobility and rapidly changing needs that traditional wireline and Ethernet can simply not address in a cost-effective way. This is coupled with the rapid evolution of the cloud itself which provides unlimited computing power and storage at a decreasing cost thus enabling cloud-managed Wi-Fi to become a reliable and viable solution.

In this short paper, we argue that the benefits of cloud Wi-Fi surpass its real or perceived limitations. These benefits include but are not limited to: simpler and faster network deployments, lower CAPEX, greater scalability, better reliability and agility, as well as easier maintenance and troubleshooting. The perceived limitations of cloud-managed Wi-Fi which include concerns around the lack of security and privacy or business continuity are also discussed.

The natural candidates to cloud-managed Wi-Fi include large distributed enterprises with many locations and small and medium business with insufficient or no IT staff to manage their Wi-Fi. However, we make the case that even large enterprises without multiple remote locations such as universities and campuses are great candidates to benefit from a transition from on-premises WLAN management to cloud-managed WLAN architectures.

For organizations who decide to switch to cloud-managed Wi-Fi, the biggest challenge is the appropriate selection of a cloud service provider that can meet the specific needs of the organization. To help organizations with this decision, this paper presents several advantages of Mojo Networks, an award-winning cloud-managed Wi-Fi service provider, such as their machine learning (ML) and artificial intelligence (AI) driven approach, their selection of powerful and inexpensive APs, and their dedication to open standards.

1. Towards an Agile Cloud WLAN

Since the first Wi-Fi standard was released almost twenty years ago, Wireless Local Area Networks (WLANs) have become an increasingly popular form of networking technology. Today, Wi-Fi is a critical and ubiquitous aspect of enterprises of all sizes and industries, furthered by the swelling usage of Wi-Fi enabled BYODs such as smartphones, tablets, laptops, and wearables.

For many businesses, Wi-Fi is mission critical to operational success. While home users may tolerate a Wi-Fi outage (albeit not without frustration), schools, hospitals, corporations, and many other organizations cannot. Enterprise network architecture reflects this criticality, as differing needs demand different solutions.

In fact, users have been improving the architecture of their WLANs since their beginning, from when Access Points (AP) were the primary network element, to the current era of cloud management and distributed control. We've seen five generations of WLAN architecture, spurred by changing user needs and updated Wi-Fi standards and chipsets. Before we describe these five generations, let's look at the history of the Wi-Fi standard itself.

1.1 Evolution of IEEE 802.11

The world's first introduction to Wi-Fi was in 1997, with the Institute of Electrical and Electronics Engineers' (IEEE's) release of the IEEE 802.11-1997 wireless standard. This standard provided up to 2 Mbps and operated in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band, which is still used today for Wi-Fi and other wireless technology. The standard didn't really catch on until 1999, with the release of the 802.11b amendment and the increasing availability of compatible devices, including the first laptop with Wi-Fi capability, the Apple iBook, which had an optional Wi-Fi card slot that was branded "AirPort". In 2000, the name "Wi-Fi" was chosen to brand the wireless technology, edging out options including "DragonFly" and "FlankSpeed" (Anonymous, 2004).

Since the new millennium, the Wi-Fi standard has been updated many times to keep pace with changing wireless needs, most notably increasing demands for faster wireless speeds. The first Wi-Fi standard offering the possibility of gigabit wireless speeds was IEEE 802.11ac, released in 2013, which operated in the 5 GHz band and provided data rates up to 1.3 Gbps (Cisco, 2017). Since then, the IEEE has been working to define the 802.11ax standard, which will be better suited to dense wireless networks (among other advantages), and is slated to be released in 2019 (IEEE Task Group AX, 2017).

1.2 Management, Control, and Data Planes

Before discussing the evolution of WLAN architectures, it will be helpful to define the concept of planes. In this context, the word plane can be thought of a set of functions and/or information necessary for some aspect of a network. There are three planes discussed in networking: the control plane, the management plane, and the data plane.

The control plane of a network architecture involves those functions by which network elements (e.g., a router) interact with neighboring elements. The control plane is thus responsible for determining routing information and carrying signaling traffic. The management plane is a subset of the control plane, and carries administrative traffic through the network. This plane includes functions for monitoring devices and their performance. Lastly, the data plane (also called the forwarding plane) is focused on forwarding packets of information through the network. This plane carries the network user traffic (Rouse, 2013) (Salisbury, 2012) (Pepelnjak, 2013).

Management Plane:

- Defined by administrative network management, administration, and monitoring.
- The functions of the management plane within an 802.11 WLAN are as follows: WLAN configuration, WLAN monitoring and reporting, WLAN firmware management
- A centralized network management server can be used to push both configuration settings and firmware upgrades to network devices.

Control Plane

- Consists of control or signaling information and is often defined as network intelligence or protocols.
- Some functions of the control plane within an 802.11 WLAN are as follows: RRM (Radio Resource Management), Dynamic RF, Roaming mechanisms, QoS, Load balancing, Band steering, Mesh protocols, Application Visibility and Control
- For example, in the case of Mojo Networks, the control plane also oversees various aspects of performance, scalability, client steering and application based traffic prioritization for voice and video.

Data Plane

- The data plane, also known as the user plane, is the location in a network where user traffic is actually forwarded.
- A standalone AP handles all data forwarding operations locally.
- In a WLAN controller solution, data is normally forwarded from the centralized controller, but data can also be forwarded at the edge of the network by an AP.
- Each vendor has a unique method and recommendations for handling data forwarding.

1.3 Five Generations of WLAN Architecture

Though the Wi-Fi standard remains an integral part of wireless network technology, it must be complemented by the appropriate hardware and network architecture. In the early days of WLANs, standalone APs served as the primary networking element. In this architecture, APs were referred to as “autonomous” and lacked an external controller. This architecture is still useful today in-home Wi-Fi networks, but is unsuitable for most other environments and mobile needs. Autonomous APs comprise the first generation of WLAN Architecture (Aerohive Networks, 2015).

The problem with autonomous APs is that, with no controller, each AP must be managed and configured independently. While not a problem for small home networks, this approach does not scale to enterprise environments with multiple APs (Avaya, 2016). Thus, the second generation of WLAN introduced a centralized controller responsible for managing “thin” APs, so called due to their dependence on the central controller. Though this allowed for easier management of the APs, this architecture suffers from several drawbacks: it's expensive to implement, as controllers are often costly and each AP must have a cabled connection to the controller; it's not very resilient, as the controller serves as a single point of failure for the network; and it's still not very scalable, as controllers are limited by a maximum capacity (Aerohive Networks, 2015) (Avaya, 2016).

The third generation of WLAN architecture saw the introduction of hybrid solutions, in which virtualization and more intelligent APs served to address some of the problems of previous architectures. Some architectures of this generation saw APs connecting to a master AP serving as a controller, which was managed in turn by a data center controller. Another option saw the controller embedded in access layer switches and firewalls to reduce the number of physical components of the network. While hybrid solutions offer greater network flexibility than previous architectures, they too have downsides: for example, a single AP acting as a controller cannot offer the same level of processing power as a dedicated physical or virtual controller (Aerohive Networks, 2015).

More recently, wireless networks have begun using the cloud to centralize management of WLANs. The fourth generation of WLAN architecture saw WLAN vendors begin providing hosted controller services for an annual fee. While this approach still utilizes a centralized controller, it eases the hardware burden on organizations and reduces network costs. However, cloud controllers maintain the drawback that, if the connection to the cloud controller is lost, the user's network will be disrupted. This could also happen if the user forgets to renew their controller license. In this architecture, the control and management planes are hosted in the cloud, whereas the data plane is hosted in the APs. (Aerohive Networks, 2015).

The fifth and latest generation of WLAN architecture removes the pain point of WLAN controllers with the introduction of distributed control. This scheme, enabled by increasing computer processing power and lower hardware costs, sees intelligent APs working together to eliminate the need for dedicated WLAN controllers. By distributing control functionality across all APs in the network, you can improve upon the fourth-generation architecture in several ways: you eliminate the single point of failure of a cloud controller, you save the cost of controller licenses by using free control protocols, you reduce architecture complexity, you eliminate traffic bottlenecks, and you have much more flexibility to scale the network to increase coverage or compute power. In this architecture, user management of the network can still be achieved through the cloud, where the management plane resides. Both the control and data planes in this architecture reside at the AP level (Aerohive Networks, 2015) (Alcatel-Lucent Enterprise, 2017).

In fact, there are today there are two iterations of cloud-managed Wi-Fi:

1) <u>Control & management planes are in the cloud</u>, ex: Cisco-Meraki while the data plane resides in the access point. This approach involves the risk of losing the ability to manage and control the access points if the connectivity is lost which may is unacceptable for most larger enterprises.
2) Only the <u>management plane</u> is based in the cloud while control and data reside in the edge/access point. Companies such as Mojo Networks and Aerohive favor this approach because access points can continue to run even if connectivity is lost.

1.4 One Size Cloud Does Not Fit All

When it comes to the cloud, there are various options available to enterprises depending on their size and ability to manage complex architectures.

An organization can use "public cloud" servers like Amazon AWS, Microsoft or Google. In all of these cases, the same set of data and computing applications are stored on the cloud provider's servers and are accessible to multiple users via the internet. This solution is usually employed by small and medium enterprises.

The second option is to use an on-premises solution (also known as a "private cloud"), which stores data and applications locally on an organization's own servers and makes it accessible to multiple users through internal networks over which they have more control. This is usually a more expensive solution more relevant for larger organization with deep pockets. The on-premises computing and data storage approach, on the other hand, requires expertise in server setup and maintenance, security and in some cases application development.

The third option is called a hybrid cloud option which consists in building an on-premises data storage system that hosts data in a Network Attached Storage device and connects to users over an internal network. Hybrid clouds can give multiple users access to both locally stored content and periodic connections to the internet for downloads. Hybrid cloud architecture is the integration of on-premises resources with cloud resources. For most organizations with on-premises technology investments, operating in a hybrid architecture can be a necessary part of cloud adoption as migrating legacy IT systems takes time.

1.5 The importance of APIs

API (Application Programming Interface) is a software interface that exposes the services and data of one application to the programmatic control of another. APIs facilitate the data and command interchanges between different programs and different tiers in a cloud-based solution. APIs are the digital glue that holds the applications and systems together.

In the Wi-Fi context, APIs enable the creation of an ecosystem consisting of the best of breed software solutions to develop around a platform. For example, as access point vendors focus on the infrastructure, they can integrate guest Wi-Fi analytics and monetization platforms for specialized software vendors thus enriching the value of the integrated solution. APIs in the WLAN can be anything that is relevant to adding value to the WLAN architecture: IoT applications, location based services, testing, big data, advertising, captive portals, etc.

1.6 Towards Open Standards

The OCP Foundation is a rapidly growing global community of technology leaders working together to break open the black box of proprietary IT infrastructure to achieve greater choice, customization, and cost savings. The mission is to apply the benefits of open source to hardware and rapidly increase the pace of innovation in, near and around the data center and beyond. For Wi-Fi systems, this means the creation of an open ecosystem of interoperable Wi-Fi software and hardware, including access points as the real value for customers is created at the silicon and software levels. The hardware brings little value other than the design and assembly of standardized parts. This is an important evolution which will benefit customers who have been locked-in with high prices on the hardware side by equipment vendors who have championed proprietary and closed systems

2. Drivers for moving Wi-Fi to the Cloud

The trend of WLAN architectures has moved towards the cloud for centralized management. With the introduction of distributed control, the cloud no longer offers a centralized controller representing a single point of failure, but rather a central dashboard for understanding and managing the network. In this section, we will discuss the advantages of cloud-managed Wi-Fi, beginning with a brief introduction to the cloud itself.

2.1 The Power of the Cloud

The cloud is best understood in terms of its physical relation to computing devices. In the second generation of WLAN architecture, with centralized controllers, the controllers are local hardware. They are in physical proximity to the network they manage. Increasingly, this physical proximity is being referred to as the "edge" of a network (Polsonetti, 2017). In contrast to the edge, the cloud is physically remote from the data it acts upon. This is exemplified by the fourth generation of WLAN architecture, in which an off-site cloud controller provides management services for a WLAN.

Consider the example of cloud storage services such as Dropbox, Google Drive, Microsoft OneDrive, or Apple iCloud. Users of these services create data on their local devices, such as computers, tablets, or phones, yet the data is not stored on these devices. Rather, the data is sent over the internet to a remote data center—the cloud. When the user wishes to access their data again, it is sent back over the internet to their local device.

Cloud computing introduces a significant shift in how technology is obtained, used, and managed. It also shifts how organizations budget and pay for technology services. Cloud computing benefits organizations by giving them the ability to trade capital expense for variable expense, gain advantage from massive economies of scale, make agile capacity decisions, increase business speed and agility, stop spending money running and maintaining data centers, and go global in minutes.

The advantages of using the cloud for services include unlimited data storage and computing power which can be added on demand to reflect changing needs and at a fraction of the cost of investing in one's own hardware. Enterprises and consumers alike are increasingly relying on cloud services to meet all aspects of their computing needs. Public cloud platforms, business services, and applications (software-as-a-service [SaaS]) will grow at a 22% CAGR between 2015 and 2020, reaching $236B according to Forrester Research.[1]

One important driver for cloud computing adoption includes a sharp decline in the pricing. Compared to the price trend of overall Computing Products (hardware and software), Cloud

[1] The Public Cloud Services Market Will Grow Rapidly To $236 Billion In 2020, Forrester, 2016

Computing Services have experienced a slightly sharper price reduction trend over the years.[2] According to Tariff Consulting's (TCL)'s "Pricing the Cloud 2 -- 2016 to 2020 report" the average entry-level cloud computing instance now costs around $0.12 per hour reflecting the intense competition between public cloud computing providers, and the rapid product innovation that is taking place among the key worldwide platform providers such as AWS, Microsoft Azure and Google. The company predicts public cloud pricing will fall by a further 14% between now and 2020.

2.2 Soon all wireless in the office?

As the modern workforce has become more mobile, businesses have started to rely more and more on wireless networks, with many questioning whether the traditional Ethernet connection has become outdated. Some organizations such as Microsoft are even evaluating turning their Ethernet dark and going all wireless to enjoy substantial cost savings from maintaining a wireline network. Such a wireless network must be rightsized, secure, ubiquitous, and support BYOD.

By getting rid of their legacy wired Ethernet network, enterprises are looking also for substantial savings from having to maintain a parallel network less and less relevant as new high-end laptops don't even come with an Ethernet port anymore while workers who are increasingly mobile rely more and more on their mobile devices such as smartphones and tablets. Moreover, all wireless offices are more agile to change and can adapt to the business changing needs more rapidly than wireline.

Other benefits of implementing an all-wireless office include removing allocated desks and offices in favor of hot-desks and meeting spaces that support mobile devices which can result in reduction of the cost in floor space per person and increase productivity.

There is also a cultural shift towards businesses using cloud-based services as part of their digital transformation. Enterprises in all sectors. Recent studies indicate that 93 Percent of Organizations Use Cloud-Based IT Services[3] such as Cloud storage and file sharing, Cloud computing/infrastructure as a service (IaaS), and Cloud-based productivity suites.

2.3 Benefits of Cloud-Managed Wi-Fi

There are many benefits to moving the Wi-Fi management plane to the cloud, just as there are many advantages of using cloud services for data storage, security services, software tools, and other services. Broadly, the cloud offers six main benefits:

1. Scalability and flexibility: Services can be easily modified to reflect changing needs of the user. For example, if you run out of storage space in Dropbox, you can purchase more and have it available instantly.
2. Measuring and monitoring: Service usage can be measured and made available to the user and service provider, allowing for the optimization of resource usage.
3. User self-service: Users can provision computing resources and capabilities as needed, without requiring the intervention of IT staff.

---

[2] Price trends for cloud computing services, 2016, Wellesley College, Honors Thesis, Liang Zhang
[3] http://www.spiceworks.com/marketing/diving-into-IT-cloud-services/report/.

4. Resource pooling: Computing resources can be dynamically shared among multiple end-users based on their individual requirements.
5. Accessibility: Since cloud services are accessed over the internet, they are available through a range of connected devices, including smartphones, tablets, and computers.
6. Multi-tenancy: The multi-tenant model of cloud computing sees users sharing a single operational instance of the cloud infrastructure, which enables the scalability of the cloud while maintaining always-on reliability of cloud services (Wainewright, 2010).

These six general characteristics listed above carry over to cloud management of WLANs, bringing the advantages of the cloud to the management of enterprise or consumer wireless networks. In addition, moving to cloud-managed Wi-Fi provides several extra benefits, such as reduced costs and network agility, that are not inherent to the cloud itself.

We will now examine some of the reasons why companies should consider transitioning to cloud networking (The Benefits of Cloud Networking, 2015) (Zyxel, 2016):

- Reduced capital expenditure (capex)

  Since management hardware is hosted by the cloud service provider, businesses no longer must invest upfront capital in building their own networks. Instead, companies simply pay an annual or monthly subscription fee in a pay-per-use model. Additionally, space and utility costs will be saved by eliminating energy-hungry hardware.

- Reduced operational expenditure (opex)

  Since cloud service providers take care of all hardware and software updates and upgrades, businesses can save the expense of hiring dedicated IT staff to manage and maintain wireless networks.

- Less downtime

  For the same reasons, organizations will experience less network downtime resulting from updates and upgrades to network infrastructure, as these services are handled by the cloud provider.

- More productivity

  Because of the eliminated network management responsibilities, IT staff will be available for other tasks, and other employees will not have to deal with productivity-affecting network downtime.

- Bring Your Own Device (BYOD)

  Since cloud services can be accessed by any device with a Wi-Fi connection, cloud-managed Wi-Fi greatly simplifies the possibility for employees to utilize their own mobile devices (BYOD), as well as work from home or on the road.

- Greater scalability

  Because cloud-managed networks can handle an unlimited number of APs, organizations can extend their coverage and/or easily add new sites without having to purchase and manage any additional hardware controllers. Cloud-managed Wi-Fi thus enables extremely agile wireless networks.

- Quicker deployment

  With cloud-managed Wi-Fi, deploying a new or extended network is as easy as a few clicks, and as fast as a few minutes. There is no more need to spend time purchasing, installing, and configuring network infrastructure, saving IT staff and end-users hours, days, or even weeks of waiting for the network to be deployed.

- Greater security

  Moving to cloud Wi-Fi shifts the burden of network security from your organization to the cloud service provider, and as such, cloud providers are incentivized to offer the best possible security features. These include encryption, authentication, malware protection, data loss protection, firewalls, and more. In fact, many companies are moving to cloud services specifically because the security capabilities of large cloud providers vastly exceed those of their own organizations (Alba, 2016).

- Remote management

  Using cloud-managed Wi-Fi offers network administrators greater management capabilities. Since cloud services can be accessed from anywhere, the wireless network can be managed from on-site, from home, or from any other location with a wireless connection.

2.4 A comparison with on premise Wi-Fi

Table 1 presents a comparison of several features of network management for each of these architectures (The Benefits of Cloud Networking, 2015) (Zyxel, 2016) (Froehlich, 2017).

Feature	Cloud management	On-premise management
Fine-grain control	CON: Some organizations may require fine-grain control over every aspect of their wireless networks. Though cloud-managed Wi-Fi is continually increasing in its capabilities, it cannot match the granularity achievable with on premise WLAN architectures.	PRO: Being able to choose, install, and configure network hardware and software gives IT staff complete control over every aspect of their WLANs. If this level of fine-grain control is necessary, on premise WLAN architectures will be more suitable than cloud management.
Scalability	PRO: The use of cloud-managed Wi-Fi enables unlimited network flexibility, as organizations can extend their networks as needed without having to purchase and set up additional infrastructure hardware. Cloud Wi-Fi enables agile wireless networks.	CON: On-premise WLAN architectures necessitate costly infrastructure upgrades to scale the network. In some cases, hardware and space limitations may place a cap on possible network expansion; for example, network controllers can only support a finite number of APs.

Feature	Cloud management	On-premise management
Hardware availability	CON: Like the above, some cloud-managed services do not provide support for certain hardware such as specific APs or antennas. This can be problematic in areas of high obstruction or interference where certain hardware options become necessary.	PRO: With no limitations on supported hardware, organizations can choose the best available hardware for their specific requirements unencumbered by cloud provider constraints.
Maintenance	PRO: One of the biggest pros of cloud-managed Wi-Fi is that all maintenance, such as hardware and software updates, is performed by the cloud service provider. This saves both time and money by eliminating the need for IT staff to perform these tasks.	CON: On-premise WLAN architectures require on-premises maintenance, which must be performed by dedicated IT staff. This maintenance can result in costly downtime and draws IT focus from other important tasks.
Connection confidence	CON: Since cloud services rely on an internet connection, your organization's confidence in constant internet connectivity is an important factor in choosing a WLAN architecture. If your organization can't achieve internet redundancy, a loss of connection to the cloud will disrupt your WLAN and result in network downtime.	PRO: Because a connection to the cloud is not necessary to manage your organization's WLAN, an internet outage does not represent a point of failure for your network management. If internet redundancy cannot be achieved, on premise WLAN management may be the best option for your organization.
Ease of deployment	PRO: Managing your network from the cloud enables easy and quick network deployment, as well as a single interface to manage geographically dispersed WLANs.	CON: With on premise WLAN architectures, network deployment is a complex process that requires individually deploying and managing network infrastructure across all sites. Compared to cloud-managed Wi-Fi, on premise Wi-Fi is both more difficult and more expensive to deploy and maintain.

Table 1 - Pros and cons of cloud-managed and on-premise WLAN architectures

2.5 Who should consider moving to Cloud Wi-Fi?

As we've seen, both cloud-managed and on premise WLAN architectures have advantages and disadvantages. As always, organizations must choose the option that works best for their specific needs. In this section, we'll discuss some of the criteria that will help determine which organizations would benefit from a transition to cloud-managed Wi-Fi.

All organizations who have an on-site controller can consider moving away from on premise Wi-Fi management.

- Organizations with multiple sites who manage WLANs across several geographically diverse locations, such as distributed enterprises or large business or university campuses.
- Organizations with limited IT staff maintaining an on premise WLAN architecture requires knowledgeable and readily-available IT staff to perform updates, troubleshoot network problems, and manage the network. For organizations with limited IT staff, such as small and medium-sized businesses (SMBs), offloading network management to the cloud service provider is an effective way to overcome this limitation.
- Organizations with changing/elastic network needs. Because of the ease of deployment and scalability offered by cloud-managed Wi-Fi, organizations using cloud services are not limited by on premise infrastructure. With a pay-as-you-grow model, these organizations can scale their network up or down as needed, without having to guess as to their future requirements.
- Organizations that encourage or require members to use their own personal devices (BYOD), such as university Wi-Fi networks, will benefit immensely from cloud-managed Wi-Fi, as it makes it simple for users and guests to join the WLAN.
- Organizations that are increasingly relying on Wi-Fi as the primary, or even the exclusive, method for their employees to access mission critical enterprise applications. Cloud managed Wi-Fi can make networks more reliable, higher performing, and reduce "time to resolution" when problems do arise.

3. Fears and Myths about Cloud-Managed Wi-Fi

Organizations that are considering transitioning to cloud-managed Wi-Fi have expressed some concerns, some justified and many based on misconceptions about the risks associated with managing Wi-Fi from the cloud:

- Security and Privacy

  Enterprises who manage customer data are rather sensitive with how data is protected from intrusion. Obvious examples include financial institutions or law firms and government agencies. These organizations are often wary that moving to cloud-managed Wi-Fi will expose them to data breaches more easily. This is a myth as the cloud has become quite mature and secure now.

- Business Continuity

  Many organizations cannot afford to lose any data resulting from human error or natural disasters, and must ensure data backups happen regularly. Organizations that demand business continuity must therefore ensure their cloud service provider has the appropriate measures in place to preserve networking data (The Benefits of Cloud Networking, 2015). This is a myth since cloud managed WIFI vendor offer very high reliability with full redundancy including at the data center. A service level agreement (SLA) of 99.99% uptime of the cloud service can help reduce the fear of downtime.

- Compliance

  Many organizations' IT departments must comply with regulatory measures such as HIPAA (Health Insurance Portability and Accountability Act) or PCI DSS (Payment Card Industry Data Security Standard). If this is the case, these organizations will have to ensure their compliance with these regulations is not impacted by switching to cloud-managed Wi-Fi.

- Localized cloud

  Some organizations may require, either for self-imposed rules or to comply with governmental regulations, that cloud servers be localized to their geographic region. When switching to cloud-managed Wi-Fi, these organizations must ensure their cloud provider offers a localized datacenter (The Benefits of Cloud Networking, 2015).

Considering Mojo

Mojo Networks is an award-winning cloud-managed Wi-Fi services provider specializing in enterprise WLAN solutions (Mojo Networks, 2017). One of Mojo's biggest differentiating features is the utilization of machine learning (ML) and artificial intelligence (AI) in the management of wireless networks. These techniques enable wireless networks to learn patterns, make predictions, and improve themselves automatically, in a paradigm that Mojo labels Cognitive Wi-Fi. ML and AI features of Mojo Aware, Mojo's Cognitive Wi-Fi platform, include real-time insights into network client devices, network baselining, root cause analysis, automatic packet capture, network profiling, and intelligent RF optimizations (Mojo Networks, 2017).

Furthermore, Mojo Networks values interoperability and so is devoted to open standards and non-proprietary hardware. To bring this value to their customers, Mojo Networks offers a series of low-cost yet highly capable APs to enable the highest performance of your organization's WLAN, placing value on the service they offer rather than the hardware necessary to support it (Mojo Networks, 2017). Mojo's APs are sold at cost, eschewing the 65-70% markup generally taken on AP sales from other providers (Tech Field Day, 2017). Despite this, Mojo's APs are of the highest quality. Mojo's C-130 AP has even received an award for the best new networking product for the higher education market, as it provides two 4x4 802.11ac Wave-2 access radios and an additional 2x2 dual-band third radio for dedicated RF visibility. This feature makes the C-130 an ideal AP for high-density networks such as those found in large schools and university campuses (Phanse, 2016).

Mojo's APs can be configured to work with any service provider, aligning with Mojo's mission to eliminate proprietary vendor hardware. In the same vein, Mojo is continually working with other cloud providers to enable interoperability of their hardware and software. Mojo also offers an extensive web-based API built upon a RESTful architecture. This is the only fully-featured API in the industry today, and it allows network operators to build their own applications to connect with their existing systems to serve their unique requirements.

Lastly, Mojo Networks provides each of the benefits of cloud-managed Wi-Fi discussed in this paper, with best-in-class security, scalability, reliability, performance, extensibility, and network visibility (Mojo Networks, 2017).

Conclusion

In this paper, we’ve discussed the evolving nature of WLAN architectures and the recent trend towards managing wireless networks through the cloud. We’ve explored the benefits of cloud-managed Wi-Fi, including cost savings and ease of deployment. Organizations of any size with dynamic network needs, limited IT staff, and/or distributed sites are among those who stand to benefit the most from a transition from on-premises WLAN management to cloud-managed WLAN architectures. Finally, we discussed several advantages of Mojo Networks, a cloud-managed Wi-Fi service provider with an award winning Cognitive Wi-Fi platform and selection of powerful APs.

About the Author

Adlane Fellah, is the CEO of Maravedis, a leading wireless analyst firm, and Wi-Fi 360, the only content marketing agency dedicated to the Wi-Fi industry. Mr. Fellah authored various landmark reports on Wi-Fi, LTE, 4G and technology trends in various industries including retail, restaurant and hospitality. He is regularly asked to speak at leading wireless and marketing events and to contribute to various influential portals and magazines such as RCR Wireless, 4G 360, Rethink Wireless, The Mobile Network, Telecom Reseller, just to name a few. He is a Certified Wireless Network Administrator (CWNA) and Certified Wireless Technology Specialist (CWTS).

About Maravedis

Maravedis is a premier wireless infrastructure analyst firm. Maravedis focus on broadband wireless technologies (including 5G, LTE, Wi-Fi, Small Cells) as well as industry spectrum regulations and operator trends. Since 2002, clients have been able to access Maravedis technology, spectrum and market intelligence through research services which include disruptive reports, webinars, online databases, analyst support and briefings as well as custom consulting engagements.

References

Aerohive Networks. (2015). Controllers, Cloud, & Cooperative Control Whitepaper. Sunnyvale: Aerohive Networks.

Aerohive Networks. (2015). The Benefits of Cloud Networking. Sunnyvale: Aerohive Networks.

Alba, M. (2016, July 21). Companies Are Moving to the Cloud to Avoid Cybersecurity Risks. (ENGINEERING.com) Retrieved October 15, 2017, from https://www.engineering.com/IOT/ArticleID/12713/Companies-Are-Moving-to-the-Cloud-to-Avoid-Cybersecurity-Risks.aspx

Alcatel-Lucent Enterprise. (2017). Distributed Wi-Fi control architecture. Alcatel-Lucent Enterprise.

Anonymous. (2004, June 10). A brief history of Wi-Fi. (The Economist) Retrieved October 14, 2017, from http://www.economist.com/node/2724397

Avaya. (2016). The Evoltuion of WLAN Architecture. Retrieved October 14, 2017, from https://www.avaya.com/en/documents/the_evolution_of_wlan_architecture_dn7858.pdf?t=0

Cisco. (2017, August 25). 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. (Cisco) Retrieved October 14, 2017, from https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html

Froehlich, A. (2017, April 24). WLAN Architecture: Cloud-Managed Vs. On-Premises. (Network Computing) Retrieved October 15, 2017, from https://www.networkcomputing.com/cloud-infrastructure/wlan-architecture-cloud-managed-vs-premises/656949372

IEEE Task Group AX. (2017, September). Status of Project IEEE 802.11ax. (Institute of Electrical and Electronics Engineers) Retrieved October 14, 2017, from http://www.ieee802.org/11/Reports/tgax_update.htm

International Data Corporation. (2017, April 6). Worldwide Cloud IT Infrastructure Spend Grew 9.2% to $32.6 Billion in 2016, According to IDC. (International Data Corporation) Retrieved October 14, 2017, from https://www.idc.com/getdoc.jsp?containerId=prUS42454017

Mojo Networks. (2017). About Mojo Networks. (Mojo Networks) Retrieved October 15, 2017, from https://www.mojonetworks.com/about-us

Mojo Networks. (2017). Cognition Plane. (Mojo Netowkrs) Retrieved October 15, 2017, from https://www.mojonetworks.com/products/cognitive-cloud-wifi/cognition-plane

Mojo Networks. (2017, October 11). Mojo Networks Recognized as Enterprise WLAN Solution Provider of the Year. (Mojo Networks) Retrieved October 15, 2017, from https://www.mojonetworks.com/about-us/in-the-news/579-mojo-networks-recognized-as-enterprise-wlan-solution-provider-of-the-year

Pepelnjak, I. (2013, August 13). Management, Control and Data Planes in Network Devices and Systems. (ipSpace) Retrieved October 19, 2017, from http://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html

Phanse, K. (2016, December 16). Mojo Networks' C-130 is Gold. (Mojo Networks) Retrieved October 15, 2017, from http://blog.mojonetworks.com/mojo-networks-c-130-is-gold

Polsonetti, C. (2017, April 17). Where exactly is the network edge? (Control Design) Retrieved October 14, 2017, from https://www.controldesign.com/articles/2017/where-exactly-is-the-network-edge/

Rouse, M. (2013, January). plane (in networking). (WhatIs.com) Retrieved October 19, 2017, from http://whatis.techtarget.com/definition/plane-in-networking

Salisbury, B. (2012, September 27). The Control Plane, Data Plane and Forwarding Plane in Networks. (NetworkStatic) Retrieved October 19, 2017, from http://networkstatic.net/the-control-plane-data-plane-and-forwarding-plane-in-networks/

Tech Field Day. (2017, July 26). Mojo Networks Mission with Rick Wilmer. (Tech Field Day) Retrieved October 19, 2017, from https://www.youtube.com/watch?list=PLinuRwpnsHadN2iQ-GDhNUfCb0oCEmaas&v=PrAo2xqifl0

Wainewright, P. (2010, September 30). Defining the true meaning of cloud. (ZDNet) Retrieved October 14, 2017, from http://www.zdnet.com/article/defining-the-true-meaning-of-cloud/?tag=mantle_skin;content

Zyxel. (2016). On-premises vs. Cloud-managed WLAN: Which one to go for. Zyxel Communications Corp.