SEVEN MYTHS OF CONTROLLER-LESS WIRELESS LANS

Vendors of controller-less WLANs are making extravagant claims for their products. But how much is reality and how much is hype?
Table of Contents

Executive Summary ........................................................................................................... 3
Introduction—Controller-Less WLANs: An Interesting but Ultimately Limited Architecture. ................................................. 3
Myth No. 1: Controller-less WLANs are controller-less ................................................................................................. 3
Myth No. 2: Controller-less WLANs are easier to deploy .............................................................................................. 4
Myth No. 3: Controller-less WLANs are as secure as controller-based WLANs ................................................................. 4
Myth No. 4: Controller-less WLANs are cheaper .............................................................................................................. 5
Myth No. 5: Controller-less WLANs are as reliable as controller-based WLANs ........................................................... 5
Myth No. 6: Controller-less and controller-based WLANs offer equivalent performance ................................................. 6
Myth No. 7: Controller-less WLANs are more flexible ..................................................................................................... 6
Conclusion—Why Juniper .................................................................................................................. 6
About Juniper Networks. .............................................................................................................. 7
Executive Summary
Wi-Fi access isn’t just an afterthought for businesses today. It is an imperative that keeps employees, customers, and partners productive. With organizations instituting liberal bring-your-own-device (BYOD) policies, users need Wi-Fi access from a broad range of mobile devices. And no matter which device they choose—laptop, smartphone, tablet, or other—they must securely and reliably access the systems and applications they need for work, research, and communication.

Keeping up with this need for omnipresent, secure, and reliable wireless network access can be challenging, especially given the number of deployment options available today. In particular, a number of vendors have introduced controller-less wireless local area network (WLAN) solutions that they claim will meet the WLAN requirements of enterprises, large and small.

This white paper debunks seven myths in the marketplace about these claims, and shows why, for the majority of organizations, a controller-based WLAN solution is still the optimal one. Specifically, although the controller-less WLAN architecture eliminates the centralized physical controller, it nevertheless still requires controller functionality. Network elements that are not designed to be traffic aggregation points—such as access points (APs)—are used to control network traffic, potentially resulting in suboptimal performance and security lapses.

Introduction—Controller-Less WLANs: An Interesting but Ultimately Limited Architecture
As the WLAN market has evolved, smaller niche wireless LAN vendors have introduced a number of interesting ideas that were designed to make WLANs more reliable, secure, and resilient. Although concepts like phased array antennas, Wi-Fi arrays, and single channel architecture initially seemed compelling, they don’t meet the needs of most organizations today.

More recently, controller-less WLAN solutions from Aruba and Aerohive have garnered considerable press, but the true merits and flaws of this architectural approach have been obscured by marketing hype. A completely controller-less solution may be viable for certain small- and mid-sized business (SMB) customers who expect their deployments to remain limited and static. However, as wireless networks grow and serve more complex needs, the advantages of centralized intelligence and single point of management offered by controller-based solutions continue to be essential to the successful operation of a WLAN network.

In most use cases, organizations should continue to use controller-based WLANs in their enterprise network architectures to ensure optimal security, ease of management, highest performance, increases in deployment flexibility, and reasonable cost. When evaluating WLAN architecture for deployment, organizations should be aware of the following seven myths about controller-less WLAN solutions.

Myth No. 1: Controller-less WLANs are controller-less
As Wi-Fi networks grew in size and complexity, organizations didn’t have the resources to continue configuring access points (APs) individually. That’s why the introduction of the WLAN controller was welcomed so enthusiastically by the IT community; controller-based solutions streamlined and reduced the complexity of configuring and managing the multiple devices that comprise wireless networks.

The enterprise WLAN market is one of the fastest growing segments in the networking world today. According to IDC’s Worldwide Quarterly Wireless LAN Tracker, the enterprise WLAN market grew 14.8% year over year in the second quarter of 2013. Currently, almost all wireless networks are managed by controllers. So-called controller-less deployments have simply moved the controller function from a centralized appliance to other locations. In most cases, they have incorporated the controller functionality into the APs themselves or moved it to the cloud. For larger wireless networks, controller-less WLAN vendors offer management applications that essentially perform functions similar to those of a controller appliance. In essence, there’s a controller even within a controller-less WLAN system—you just don’t have control of it.

The point is, there is always a controller. It exists, one way or another. The controller just takes on different forms—and is paid for in different ways. Vendors that embed the controller functionality in the APs have integrated the cost of the controller into that of the APs and in the service contracts for the APs. Cloud vendors include the controller costs in the price of the virtual AP subscriptions.
Myth No. 2: Controller-less WLANs are easier to deploy

This is one of the more persistent myths. Although it’s true that initially, controller-less WLANs appear easier to set up than those with a centralized controller, the situation changes very quickly once you begin to extend your network.

In a controller-less WLAN system, you need to reconfigure your access layer with the addition of each new AP. Since it is necessary to configure all virtual LANs (VLANs) on the switch port that is needed by each new AP, your network administrator needs to configure the wiring closet switches that each new AP connects to. For example, you may have a VLAN for guest access, a VLAN for corporate access, and a VLAN for special access (such as VoIP). All these VLANs must be configured each time you add a new AP.

With a controller-based WLAN system, it is infinitely easier to add APs. The access layer is configured once at the handoff to the controller and the system manages the rest. The centralized controller provides rich functionality for automating deployment complexity, eliminating the need for frequent, error-prone changes to the access layer. You simply plug in the AP and it automatically self-configures. Expansion of your network couldn’t be simpler.

Myth No. 3: Controller-less WLANs are as secure as controller-based WLANs

Security is a top priority for network administrators. Monitoring and reacting to system-wide security events requires a holistic view of the network. This is best provided by a controller-based WLAN.

Most organizations have security policies that determine how to treat untrusted wireless traffic. Controller-based WLANs offer a very clean and elegant solution to comply with security mandates for isolating untrusted wireless traffic from the network. For instance, the architecture naturally lends itself to having all traffic terminated at the controller and transporting all guest traffic to a DMZ or firewall.

In contrast, controller-less WLANs have inefficient workarounds, such as forcing an AP to act as the approved handoff point for untrusted traffic. A controller is purpose-built for such a function. An AP, on the other hand, is specifically designed to be a single node on the network; it is not designed to function as an aggregation point. Using APs in this fashion can put an organization at risk and adversely impact performance.

For example, in a typical enterprise wireless network deployment, secure corporate access is provided to employees, while limited access is granted to guest traffic. Many organizations, for security reasons, do not allow untrusted guest traffic to interact with their network. Controllers give organizations an easy way to manage network traffic. Untrusted traffic gets tunneled to the controller and fed out of a separate physical port to the firewall or other security mechanism for inspection. An AP can then put trusted traffic instantly on the network, preventing any potential bottlenecks.

A controller-less WLAN system, on the other hand, needs to use one of the APs to provide that physical connection for guest access. Organizations need to create workarounds with the physical network to allow APs to act as tunnel termination points.

Organizations frequently choose to place greater security restrictions around wireless network segments than on the wired segments. The controller-based WLAN model gives enterprises the ability to deploy APs in limited-access network segments. By leveraging AP-to-controller tunneling, organizations can prevent exposure through unprotected network ports.

There may be regulatory needs to tunnel traffic to a specific place. For example, compliance with the Health Insurance Portability and Accountability Act (HIPAA) requires that all wireless traffic go through a central point. Organizations may also want to route traffic through a central location if they want to meter or control the bandwidth, or to shut down or disable individual APs.

In a controller-less WLAN architecture, the lack of visibility into system-wide security events provided to APs may also expose this type of system to additional security risks. Similarly, physical compromise of an AP device can risk exposing sensitive configuration data. Since each device in a controller-less system is responsible for forwarding client traffic, a stolen AP can expose the network to an attack; for example, an attacker could open a network port and gain access to the wired network. This problem would be compounded if the controller-less device required a VLAN trunk to provide access to multiple VLANs.

All of the above speaks to on-premise WLANs. Deployment of cloud-based WLAN solutions often requires significant changes to perimeter security policies. (For more on this point, see Myth No. 6.) In addition to the security risk associated with these changes, there is also the inconvenience of having to manage security by exception.
Myth No. 4: Controller-less WLANs are cheaper

At first glance, controller-less WLANs—especially cloud-based ones—appear less costly than controller-based WLANs. Certainly, the initial price tag indicates that this is the case. But doing a detailed total cost of ownership (TCO) analysis quickly refutes that claim.

When comparing the Juniper Networks® JunosV Wireless LAN Controller to an equivalent controller-less WLAN cloud-based solution, we arrived at the following numbers:

<table>
<thead>
<tr>
<th></th>
<th>Other vendor cloud-based controller-less WLAN</th>
<th>Juniper controller-based WLAN</th>
<th>Savings by going with a controller-based solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial investment</td>
<td>$572,000</td>
<td>$588,110</td>
<td>-3%</td>
</tr>
<tr>
<td>Third year</td>
<td>$717,000</td>
<td>$618,330</td>
<td>16%</td>
</tr>
<tr>
<td>Fifth year</td>
<td>$862,000</td>
<td>$648,550</td>
<td>33%</td>
</tr>
</tbody>
</table>

This comparison is based on a 500 access point deployment using 3x3, 3 spatial stream 802.11n gear. The other vendor’s controller-less solution includes cloud controller and enterprise support subscriptions. The Juniper controller-based solution employs a JunosV Wireless LAN Controller subscription, Juniper Networks Junos® Space Network Director for management, and an enterprise support subscription.

The following comparison is based on an on-premise controller-less WLAN solution from the same other vendor, again for 500 access points for an 802.11n wireless network:

<table>
<thead>
<tr>
<th></th>
<th>Other vendor on-premise controller-less WLAN</th>
<th>Juniper controller-based WLAN</th>
<th>Savings by going with a controller-based solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial investment</td>
<td>$600,999</td>
<td>$588,110</td>
<td>2%</td>
</tr>
</tbody>
</table>

This includes licenses for the vendor’s on-premise WLAN manager software and an enterprise support subscription. The Juniper cost remains the same as the previous configuration.

Controller-less WLAN systems can be more costly for the following reasons:

- The cost of the controller functionality is slipped in elsewhere in a controller-less system (in the cost of required service contracts, for example).
- The cloud model, where the management functionality is located in the cloud, requires a subscription that must be continuously renewed. Over the long haul, this model is much more expensive than simply purchasing a WLAN controller from the start.
- For non-cloud models, purchase and management of the server system for management software adds cost to the controller-less solution.

Myth No. 5: Controller-less WLANs are as reliable as controller-based WLANs

In mission-critical wireless networks, the ability to coordinate the failover and failback behavior of a complex system is critical. Ensuring high availability is a top priority of any WLAN deployment, especially on wireless networks that carry latency-sensitive traffic such as voice data. Organizations need to be confident that if an AP fails, network traffic won’t be impacted. All this is best achieved by a centrally managed controller with complete visibility into the entire WLAN system.

With a controller-based model, the controller acts as a single point of coordination for all APs. In case of a failure, the controller can orchestrate in failure mode to minimize latency. Because all session information for all wireless users is stored in the centralized controller, in the event that an AP fails, users are immediately transferred to a different AP, which can get all necessary information about those user sessions from the centralized controller.

However, in the controller-less model, the individual APs don’t have a centralized location to get the necessary user information. In an outage or AP failure in controller-less WLAN systems, cached credentials, identifiers, or client context information may be lost and would need to be reestablished on a new AP. As a result, latency can increase.

Different vendors have taken different approaches to manage this problem, but no workaround can completely eliminate this weakness in the controller-less WLAN architecture.
Myth No. 6: Controller-less and controller-based WLANs offer equivalent performance

Controller-based solutions provide options to distribute data processing to the local APs, while maintaining the benefits of centralized command and control. By removing the controller from the data path, potential performance bottlenecks are eliminated.

Although the controller-less architecture provides a similar optimized data-forwarding path, there is a sacrifice in performance, since all individual APs must also perform controller functions that are typically performed by a centralized controller.

Additionally, WLANs are heavily dependent on other components in the network: the authentication server to authenticate users, network switching to give access to VLANs, and other network management elements. Once the number of APs reaches a certain threshold, the complexity of coordinating all these components can take a performance toll, even though the user interface may mask the complexity of the tasks. A larger number of APs also results in a greater possibility of errors and increased complexity for network administrators to manage.

For example, in a controller-less WLAN system, the AP that is used as the proxy authentication server acts as the aggregation point for client authentication and must interact with every other AP in the system, resulting in less than optimal performance. Because every AP has a portal page while also negotiating other types of traffic, there is the possibility of introducing latency into the system. The larger the environment, the greater the complexity—and the possibility that performance will suffer.

Taking WLANs to the cloud introduces even more complications, as many of the network elements are on-premise. For example, Active Directory data will most likely to be located in the data center. If the WLAN controller is in the cloud, how does that controller communicate through the public Internet, firewalls, and security policies so that users can be authenticated? The way that the control process is implemented can have very real performance implications.

Then there are the performance implications of tunneling traffic to APs, devices that were not purpose-built for moving data. APs were not designed to support high-scale tunnel traffic. In contrast, centralized controllers have dedicated hardware that makes them extremely efficient at moving traffic through the network.

Performance can also be impacted when users roam across multiple access points on a campus. In a controller-less model, APs are grouped into “pods” to streamline roaming. If these pods get too large and unwieldy, organizations will see performance degradations. Moreover, individual AP pods may be efficient at managing roaming, but when users cross pod boundaries, additional performance issues arise; the session will not be seamless for the user and their connection to the WLAN will likely be interrupted. Managing roaming in a controller-less WLAN is simply not as efficient as in a centralized controller environment where users can be moved transparently, from one AP to another, with no impact to performance.

Myth No. 7: Controller-less WLANs are more flexible

Finally, one size does not fit all when it comes to WLANs. Choose an architecture that fits your deployment. A controller-based WLAN solution offers more choices, and thus more flexibility, than a controller-less WLAN model. With a controller, organizations can choose to forward traffic locally at the APs (similar to the method used in controller-less WLANs), or they can choose to tunnel certain types of traffic back to the controller for security reasons. With a controller-based WLAN, organizations have the flexibility to mix and match these approaches as appropriate. A controller-based architecture also gives enterprises the ability to attach tunneling and local switching to user identities and roles.

With controller-based WLAN solutions, organizations also have the flexibility to adapt to many different network topologies and network layouts—precisely because the controller, rather than the individual APs, is the central point of control.

Conclusion—Why Juniper

The Juniper Networks wireless LAN solution has been a leader in controller-based WLAN since the architecture was introduced in 2002. The product line was first to market with many of the innovations associated with the “thin AP” architecture. Today, Juniper offers a broad range of WLAN deployment options for enterprises of all sizes (see Figure 1) giving you the flexibility to tailor wireless LAN service to meet all of your business needs.
To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.