



WHITE PAPER

An Extensible Platform for WLAN Service Assurance

Author: Joe Epstein, Sr. Director of Technology

TABLE OF CONTENTS

Introduction	3
Scaling the Pool of Data about Wireless Operations.....	5
Services Running on the Service Assurance Platform Today	7
Conclusion	8

Introduction

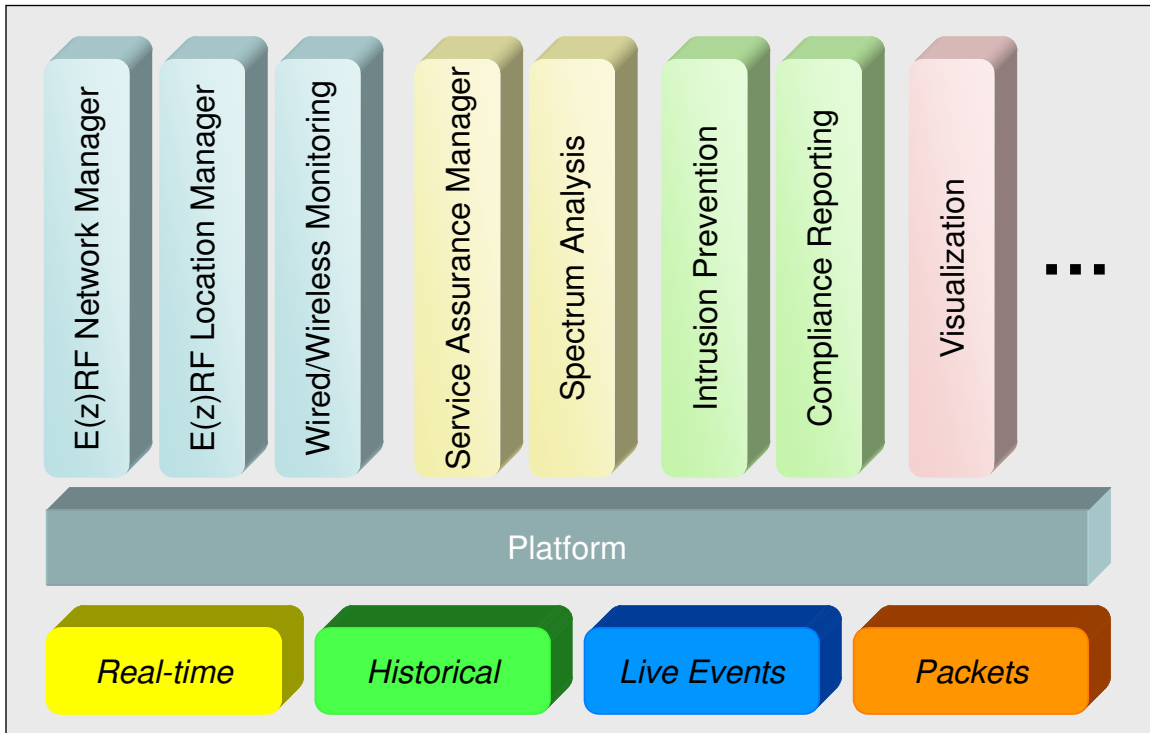
Most high-scale enterprise wireless LAN networks today start with access points and controllers, the devices which underpin the connectivity and traffic flow from users to the core enterprise IT services. Although this is enough to establish a high-performance network, the role of *operating* that network and simultaneously assuring high-quality service is something that has not been the primary focus of enterprise WLAN.

However, with the adoption of the 300Mbps 802.11n wireless technology, the role of the wireless network itself has changed from simply providing mobile connectivity to becoming the default network for a wide variety of core IT applications that were never designed to run on a wireless network. For this new network to be successful, however, the wireless network must have the same predictability and availability of the fundamental service it provides as that of the wireline network which it displaces. This new requirement, for a stable and predictable wireless network rather than one that merely provides convenient access, is driving the need for *service assurance* for wireless to the forefront.

Delivering upon the need for wireless service assurance involves introducing a wide array of new, yet critical, plug-in additions into the WLAN. These additions, primarily based on intelligent software, require both broad and deep access into the WLAN itself, as they have to not only monitor the network after-the-fact but *proactively* determine where and when the threats to service assurance lie and allow them to be addressed before those threats directly impact the wireless users. Yet, the additions must not steal necessary resources from the running access points and controllers. The identities of these new wireless-operations focused applications are quite varied. Some are old, such as wireless network management and device location tracking. Some are new and unique, such as proactive network verification and real-time spectrum interference detection and avoidance. All of them require detailed knowledge of, integration into, and interaction with the underlying wireless network, and yet they also must span the entire network without regard to the individual divisions of controllers, access points, and department-level divisions of service.

The solution to the problem of delivering these critical service assurance operations is with the introduction of the *Service Assurance Platform*.

Meru Service Assurance Platform



The Service Assurance Platform is an extensible, pluggable software platform, running on a dedicated Services Appliance, that integrates directly into the enterprise WLAN to provide the necessary foundation for hosting the set of critical service assurance software modules, yet runs separately from the controllers and access points and can operate within a different wired network or geographic location. The Service Assurance Platform provides to each software module a wealth of real-time and historical wireless network data—not just the base statistics that existing wireless network management platforms collect and expose, but live, critical wireless events for every device, along side with direct access to the contents of critical wireless packets and the ability to inject and monitor traffic directly into the WLAN.

The key to the Service Assurance architecture is that these critical services are provided in a highly-scalable manner that does not impact the operation of the wireless network. Doing so requires a complete re-think of how additional wireless services are integrated into the WLAN.

Scaling the Pool of Data about Wireless Operations

Because the critical importance wireless networks have taken on within the umbrella of IT services, providing wireless service assurance requires access to a tremendous pool of previously-unneeded data about the operation of the wireless network. This pool of data extends far beyond statistics, to include the real events each wireless device experiences, to use in client diagnostics; real wireless packets, to use in signature-based intrusion prevention and proactive network verification; real-time state, for visualization and signature-based network diagnostics; and historical state, for network management and compliance reporting.

The Service Assurance Platform is able to get access to that pool without requiring itself to be placed along the critical path of data flow (such as in access points or controllers on a link between the two) , and by reducing the actual throughput required to operate platform, by using unique, highly-scalable methods of data acquisition.

The main innovation is to move away from SNMP (and SNMP-like protocols) as the means of collecting data from controllers and access points and into the Service Assurance Platform. This doesn't mean that the availability of SNMP for your own monitoring tools is going away. Instead, just as the protocol between the access point and the controller needs to be optimized for scale first, the protocol between the controller and Service Assurance Platform needs to be optimized as well.

This optimization involves moving away from the periodic polling—or *pull*—model of aggregating operations data into a monitoring platform. Pulling data is never a good idea for high-scale systems, and for wireless, the problem of pulling data is made even worse. SNMP-like protocols work by asking for a complete set of every bit of statistics and operations data the controller has, whether or not each bit has changed or has meaningful data. This has to be done, because of the way the SNMP protocol works, as it is based on the notions of “walking” tables or pulling OIDs.

Furthermore, some bits of data are more important than others. Crucial ones, such as the signal strength of a client, may be needed far more often than less important ones, such as frame counts. However, SNMP-based wireless tools tend not to offer the ability to ask for some data more often than others.

The consequence of the pull model is that the management platform can directly impact the performance of the underlying wireless network, simply by asking for data more often than the WLAN can respond with without causing CPU loads to go up. Finding the right balance between fresh, useful data in the management platform and not overloading the system is a tough procedure to perform, and the odds are that the out-of-the-box polling interval for pull-based tools is never right.

The Service Assurance Platform aggregates the operations data more intelligently, by having the controllers and access points push data to it. And when they do so, they push only the important changes, thus greatly reducing overhead and increasing scalability, allowing applications to be designed for the Service Assurance Platform that can depend on having fresh information network-wide, enabling them to not only record and report on the data but react to it, something simply not feasible on other WLAN management platforms.

On top of this new push-based model, the type of operations information the Service Assurance Platform can gather opens up tremendously. Not only can the platform gather statistics—the SNMP style of data—but it can now gather real wireless network events. These events are not just periodic samplings of statistics, but a complete log of when each device has done something of importance to the wireless network—such as associating, authenticating with the RADIUS server, and acquiring an IP address. That information is far more valuable to diagnosing a network than simple statistics are: would you rather only know that a client's throughput (a statistic) has gone to zero over a five minute polling interval, or would you rather have a log that shows that the client disconnected from the network, then reconnected, but repeatedly failed to authenticate because of a bad password? Event logs provide the latter, and, because of the push-based architecture of the Service Assurance Platform, these events are provided automatically for every client. There is no need to delay enabling them until you need to diagnose something, out of fear of causing a network impact by enabling them. There is no such impact, and thus these events come with the platform, on for all time, maximizing your ability to diagnose yet without causing scale issues.

Beyond events, the Service Assurance Platform has access to actual packets. This access comes in two forms. The first is for monitoring or scanning the network. The Service Assurance Platform is able to slice the wireless traffic, getting insight into what is happening without burdening the system or the network by requiring a mirroring of every packet. These slices are generated intelligently, in real time, in cooperation with the access points. With this, the Service Assurance Platform can offer real-time locationing and security services.

The second form of packet access is the ability to send traffic from access points and receive them from others. This allows the Service Assurance Platform to form a closed-loop of traffic *through* the wireless network, including going over the air. Such access allows the Service Assurance Platform to perform one of the most important activities for assuring service—the ability to automatically validate the quality and level of service of the network *proactively*.

Services Running on the Service Assurance Platform Today

With the Service Assurance Platform's ability to efficiently access real-time operations data of the WLAN without interfering with it, a number of key WLAN plug-ins are available today.

- *Service Assurance Manager*: The Service Assurance Manager is the pivotal service offered on the platform. SAM proactively validates the network by creating *virtual clients* on each access point. These virtual clients co-exist with the actual clients on the wireless network, causing no disruption to service. Rather, they are created to measure service, by associating back with the wireless network through other access points and then injecting traffic back to the Service Assurance Platform. This traffic is then measured for distortions or changes to quality, allowing SAM to catch problems before users do, offering huge potential savings to the helpdesk costs by reducing the number of incoming trouble tickets.
- *E(z)RF Network Manager*: The E(z)RF Network Manager provides the wireless-specific network intelligence to determine how services are being delivered and to diagnose problems that occur. Not just the typical network manager, E(z)RF Network Manager takes advantage of the additional data captured by the Service Assurance Platform, including the event logs and additional diagnostic inferences provided by the WLAN, to provide true forensic "rewind and replay" capabilities far beyond that of simply looking at historical statistics. The overall effect is to reduce the time to insight for wireless problems, in many cases from hours or days to simply minutes.
- *E(z)RF Location Manager*: The E(z)RF Location Manager provides real-time locations of devices for use in hospitals, manufacturing, or wherever location-based services is critical. The Location Manager takes advantage of the real-time packet access to locate devices without significant delay and with greater potential accuracy, as opposed to signal-strength trilateration-based (or triangulation-based) location systems that are delayed by the SNMP polling interval.
- *Spectrum Analysis*: Having access to real-time events also allows for the Service Assurance Platform to receive notifications from the Meru PSM series of spectrum monitors, thus providing crucial alerts when network-damaging interferers (such as microwave ovens and wireless video cameras) are activated. This information is then able to be provided directly into the E(z)RF Network Manager for rewind and replay analysis and immediate WLAN response.

- Intrusion Prevention: Scalable packet access allows for wireless intrusion prevention services, using signatures to detect a wide variety of attacks on the WLAN and escalate when these problems become significant or severe.
- Compliance Reporting: By being able to aggregate the configuration and operations data for the WLAN, the Service Assurance Platform is able to host Compliance Reporting modules, to provide reassurance that the network is able to offer PCI DSS compliant services.
- Wired/Wireless Monitoring: Service Assurance includes the wired network as well, and the Service Assurance Platform is in the proper location in the network to integrate wired and wireless operations into a cohesive single-screen monitoring platform.

Conclusion

Wireless networks have matured from being a convenience-only appendix to standing front-and-center for mission-critical IT services, and this transition requires these networks to be focused around the notion of service assurance. Meru is able to offer service assurance for high-performance, high-capacity 802.11n-based WLANs using the Service Assurance Platform, which ties together innovative methods of scalable access to the WLAN and its operations data to offer a pluggable set of key modules that go well beyond network *management* to assuring the availability, quality, and security of the service itself. The maturity of wireless networks has elevated the problem from simply providing coverage with access points and controllers, to offering deep insight to the wireless network's operation itself from an additional, critical services appliance. No longer is IT limited to controlling for CAPEX for wireless; now it can take advantage of the concept of service assurance to control for the OPEX.



advanced
network
systems

For More Information,
Contact Us:

800.639.6757
sales@getadvanced.net

www.getadvanced.net