Centralized Wi-Fi Troubleshooting and RF Management

A Webtorials® Thought Leadership Spotlight™

Joanie Wexler, Moderator

Enterprise-grade Wi-Fi vendors have been hard at work enhancing their RF monitoring tools to make Wi-Fi's performance and reliability as close to Ethernet's as possible. The reason? With 802.11n offering 300Mbps connect rates per radio, Wi-Fi has become a bona fide competitor to wired Ethernet. So enterprises are moving from Wi-Fi as a "nice to have" to Wi-Fi as a mission-critical network.

Join me as I discuss with Amit Sinha, Fellow and Chief Technologist at Motorola AirDefense, what his company's Network Assurance centralized WLAN monitoring and troubleshooting capabilities bring to the wireless enterprise table.

Joanie Wexler, Moderator

Most of us know that wireless is a funky transport medium that basically must be beaten into submission with sophisticated RF monitoring and management tools in order to perform reliably. Briefly, what does Network Assurance do that's special?

Amit Sinha, Motorola

As a growing number of organizations look to use wireless LANs for more demanding applications like voice or video, administrators are realizing that managing the performance of wireless networks has become crucial to improving business operations. Unlike wired networks, where reliability of the communication medium is not as significant a problem and the availability of centralized tools results in quick turnaround of networking trouble tickets, enterprise IT often struggles with effective resolution of wireless network problems. WLAN Network Assurance solutions offer a suite of vendor agnostic WLAN analysis and troubleshooting tools that that allow organizations to proactively optimize wireless LAN performance as well as remotely troubleshoot RF or user connectivity issues.

Joanie Wexler, Moderator

But, specifically, Amit, what does Network Assurance do that's special? There are other suites of RF tools to help wireless performance from Motorola (as well as from your competitors). There are lots of names spinning about. What, specifically, does Network Assurance do that, for example, SmartRF and LiveRF, don't, if anything?

Amit Sinha, Motorola

Network Assurance is not one tool, it is a suite of tools. Tools such as LiveRF are part of Network Assurance. Network Assurance consists of tools that help analyze past, present and future wireless problems. Historical analysis tools can debug intermittent problems that happen, say at lunch time when the microwave oven is on. Tools such as LiveRF provide real-time application coverage heat maps. Then there are automatic AP Test tools that can check the wireless network as well as wired services across your deployment and flag issues proactively before users complain. Such a comprehensive toolset is unique to Motorola.

Joanie Wexler, Moderator

How does Network Assurance differ from Motorola SmartRF, another Motorola suite of RF management tools?

Amit Sinha, Motorola

Reliable WLANs require three basic components: (i) Good planning, (ii) Resilient architecture, (iii) Network assurance solutions.

Good planning tools, such as Motorola's LANPlanner, can provide application and building aware simulations that can optimize the placement of APs for optimal coverage and desired capacity.

Resilient WLAN architectures can provide access despite unpredictable RF conditions and wired network outages. Motorola's SMART RF falls under this category. It consists of algorithms embedded in the WLAN infrastructure that allows automatic adjustment of transmit power levels and frequency plans based on dynamic RF conditions and client load.

Despite best planning and self-healing WLAN deployments, you will still have the occasional network outage or user connectivity issue. This is where network assurance tools come in handy.

The Motorola AirDefense Network Assurance Solution offers a unique set of tools for vendor agnostic, WLAN performance monitoring and remote troubleshooting of RF problems. The solution uses a dedicated network of RF sensors that continuously monitor the airwaves – intelligently scanning different frequencies over time and space to detect WLAN performance problems and policy violations. Motorola analyzes traffic flow to interpret WLAN performance and to identify common characteristics that may impede network performance such as interference from neighboring WLANs, channel overlap, over-utilized APs & channels, network congestion, and performance degradation. By providing a view of all WLAN traffic, the Network Assurance tools enable network administrators to remotely troubleshoot problems, identify and respond to network mis-configurations, and monitor network availability.

Once a problem or issue is identified network administrators have two types of tools, real-time and historical, which allow them to appropriately diagnose and remediate the problem. The real-time toolset allows administrators to see what is happening in the WLAN at that given instant. Many RF issues are hard to replicate or transient in nature, and the ability to remotely and instantly visualize and analyze the user’s WLAN from a central location is valuable. The historical toolset allows administrators to analyze device specific trends over time to better understand the root cause of a problem or detect intermittent problems. The ability to remotely troubleshoot and resolve WLAN performance problems, in real-time, with access to historical data for perspective, is crucial for maximizing

the availability and ROI from a WLAN. The innovative add-on modules integrated in the Motorola AirDefense Network Assurance suite include Motorola AirDefense Advanced Troubleshooting, Motorola AirDefense Spectrum Analysis, Motorola AirDefense LiveRF, and Motorola AirDefense Advanced Forensics.

 **Joanie Wexler, Moderator**

I see that Network Assurance is a vendor-agnostic suite of monitoring tools. To play devil's advocate, how likely is it that a customer of, say, Cisco, Aruba or other enterprise-class WLAN vendor will turn to Motorola (rather than their own WLAN systems vendor or a third party without vested interests) for a centralized WAN monitoring solution?

 **Amit Sinha, Motorola**

Motorola AirDefense is currently deployed as a vendor agnostic security and performance monitoring solution in hundreds of non-Motorola WLAN deployments.

Built-in performance monitoring and remote troubleshooting capabilities are limited in WLAN infrastructure. They lack 24x7 monitoring, granular minute-by-minute information for all wireless devices, Level 1 Helpdesk optimized tools, proactive AP testing, application layer coverage analysis, etc.

As the WLAN deployment scales, the lack of robust network assurance solutions often lead to operational expenses exceeding capital costs over time. Having robust network assurance solutions will reduce support costs while minimizing wireless network downtime.

 **Joanie Wexler, Moderator**

How does Motorola decide what RF tools to integrate into its WLAN infrastructure products and which to embed in the AirDefense "overlay?"

 **Amit Sinha, Motorola**

AirDefense is integrated into Motorola WLAN. As such Motorola APs have band unlocked radios that become AirDefense sensors. Further, AirDefense is the management platform for Motorola WLAN deployments. Using its multi-vendor management capabilities, it can configure and manaage not just Motorola but also other vendor's WLAN.

 **Joanie Wexler, Moderator**

Do I need to dedicate special APs (sensors) to do 24x7 monitoring with Network Assurance? If so, how many do I need to deploy? And doesn't this get expensive?

 **Amit Sinha, Motorola**

Motorola AirDefense uses dedicated radios for 24x7 monitoring. Motorola APs have band-unlocked dual and tri-radio options where the second or third radio can become the full-time sensor. This reduces cost by eliminating the need for standalone sensors and their associated cable drops and switch ports.

If you do not have Motorola APs deployed, you can still get all the benefits of the AirDefense solution by deploying dedicated AirDefense sensors. A typical deployment has 1 sensor for every 3-5 APs.

 **Joanie Wexler, Moderator**

Can I use the same set of sensors for wireless intrusion detection and prevention scanning (WIPS) to find rogue devices?

 **Amit Sinha, Motorola**

Yes. The same 24x7 sensor provides all the AirDefense functions: (i) Security and Compliance - including rogue elimination, wireless IPS, forensics, (ii) Network Assurance.

 **Joanie Wexler, Moderator**

I see that Network Assurance supports spectrum analysis – a capability that has been announced recently by a number of WLAN vendors, seemingly following Motorola's lead. Once I discover and classify an interfering device and determine its impact on my Wi-Fi network' performance, what can I do to resolve its effects, if needed?

 **Amit Sinha, Motorola**

True. Motorola has been shipping patented, WLAN software Spectrum Analysis (SA) solutions for over 2 years. SA is just one component of a multi-pronged network assurance toolset.

SA can flag sources of interference that are affecting WLAN performance. This information can be leveraged by an administrator (manually) or the WLAN management system (automatically) to update the operating frequencies to mitigate the effects of the interference source.

 **Joanie Wexler, Moderator**

Does Network Assurance support any so-called "air-time fairness" capabilities that prevent the slowest client on the Wi-Fi network from gating overall network performance?

 **Amit Sinha, Motorola**

Airtime fairness is a WLAN infrastructure feature. The ability to "allocate" the RF medium to "slow" and "fast" clients on an equitable basis is best performed by the AP. Motorola APs support this feature.

Network assurance can monitor client behavior and provide channel capacity and airtime fairness metrics to the WLAN infrastructure to improve performance of the algorithm.

 **Joanie Wexler, Moderator**

Specifically, how can Network Assurance help enterprises achieve the QoS metrics needed to support quality voice over IP over WLAN (VoWLAN) traffic?

 **Amit Sinha, Motorola**

Motorola AirDefense includes tools such as LiveRF in the Network Assurance suite. LiveRF can monitor real-time coverage for applications such as voice and video and compare it to the original deployment design. It can automatically flag areas where voice coverage is being impacted because of noise, interference or change in building topology, based on real-time measurements.

Similarly, performance monitoring policies can be defined in AirDefense, specific to voice applications. The system then monitors the network 24x7 and generates alerts when performance thresholds are crossed.

 **Joanie Wexler, Moderator**

What's "promiscuous mode" and what are some of the benefits of supporting it?

 **Amit Sinha, Motorola**

"Promiscuous mode" is a monitoring mode for a network interface. For WLAN security and network assurance, WLAN radios need to support "promiscuous mode" packet capture capabilities so that they can have complete visibility of what is happening in the environment.

Access Points typically drop traffic where the destination address is not their wireless MAC address. This could be a serious limitation for monitoring functions.

 **Joanie Wexler, Moderator**

Just to clarify,then, promiscuous mode does NOT drop frames not addressed to the network interface on an AP/sensor? What kinds of analyses can Network Assurance do with these packets; in other words, what security or performance benefit is possible using promiscuous mode?

 **Amit Sinha, Motorola**

Yes. The ability to "see" all devices and traffic is key for security and performance monitoring. If you cannot see all traffic, you cannot detect rogue devices or attacks on the WLAN. Similarly, it is important to see all devices, weather they are associated or not, to be able to measure performance metrics such as channel utilization, etc. The WLAN RF medium is shared with lots of WiFi and non-WiFi devices. If you only see the devices that are talking to you, you will have a very limited and inaccurate view of the air space.

 **Joanie Wexler, Moderator**

Can you explain the "intelligent scanning algorithm" used by Network Assurance sensors?

 **Amit Sinha, Motorola**

"Intelligent scanning" refers to the ability of the sensor radio to dynamically adjust the frequency scanning pattern and corresponding dwell times on each channel to maximize visibility. There are many channels in the 2.4 and 5 GHz bands. Security issues can occur anywhere. Since a single radio sensor can only be on one channel at any given time, it is important that it adjust its channel scanning dynamically to avoid missing critical events. Similarly, effective performance monitoring requires the sensor radio be able to capture traffic and noise sources at the right time on the right channel.

 **Joanie Wexler, Moderator**

What do you think, in general, have been the most important recent advances in Wi-Fi monitoring and management? Any others on the horizon?

 **Amit Sinha, Motorola**

The ability to integrate 24x7 monitoring technology in WLAN infrastructure APs using band-unlocked radios was a key step in reducing cost and simplying management.

Similarly, the ability to embed spectrum analysis capabilities pervasively, using native Wi-Fi radios, without having to deploy special hardware was another innovation.

The ability to go from reactive monitoring to proactive network assurance was a big step. Leveraging sensor radios as clients to actively test WLANs from an end user and application access perspective was a leap forward.

Finally, making WLAN monitoring more application aware, instead of focusing on low level Layer 1 or 2 analysis, has also been a big advancement.

Motorola AirDefense has been a leader in the WLAN monitoring space with these disruptive innovations and will continue to do so.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.