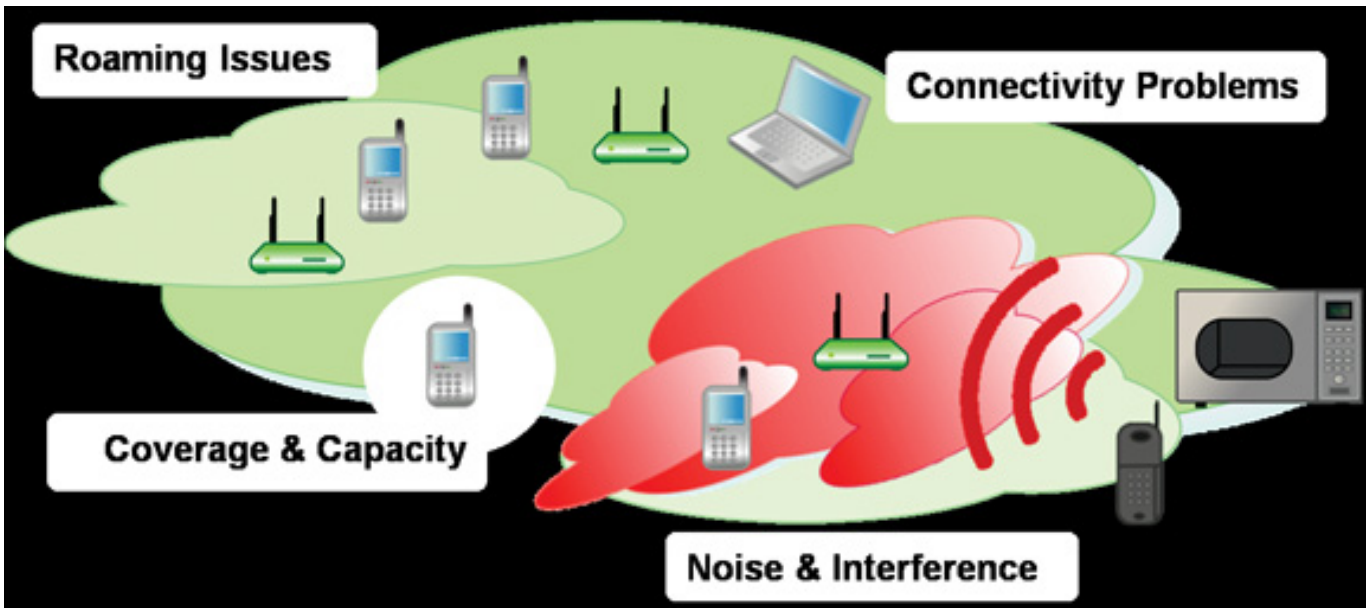
Wireless Network Assurance: Must Have Tools for Mission Critical Wireless LANs

Dr. Amit Sinha, Motorola Enterprise WLAN

Wireless Local Area Networks (WLAN) have proliferated within the enterprise. While the cost of deploying a WLAN solution has dropped over the last several years, the operational expense of maintaining and managing a WLAN continues to rise. As more and more enterprise applications and workforces migrate to wireless, the cost of troubleshooting and fixing wireless network connectivity and performance issues is increasing. WLANs use a shared, license-free, radio frequency (RF) medium for communications. The operational challenges of running a wireless network are unique and different from wired networks. Some common issues that often affect WLAN performance are:

Coverage and Capacity - WLANs typically consist of Access Points (APs) distributed across the enterprise. RF signal strength wanes as the distance from the transmitting source increases. Indoor RF propagation is strongly affected by obstacles and multipath propagation, which in turn depends on building characteristics and layout. Despite the best efforts, most enterprise deployments still suffer from coverage holes. Sometimes users experience reduced throughput from the WLAN even though they have good signal strength. This often happens when other users are taking up excessive shared bandwidth or when the AP is overloaded.



Noise and Interference - WLANs operate in the Industrial, Medical and Scientific (ISM) license-free band (2.4 GHz and 5 GHz), shared by other wireless protocols and devices such as Bluetooth, cordless phones, microwave ovens, wireless cameras, etc. Noise and interference increase packet error rate, frequently leading to reduced wireless throughput, and occasionally loss of connectivity. Another common problem in WLANs is co-channel interference, which occurs when two or more WLANs are operating on the same channel in mutual proximity.

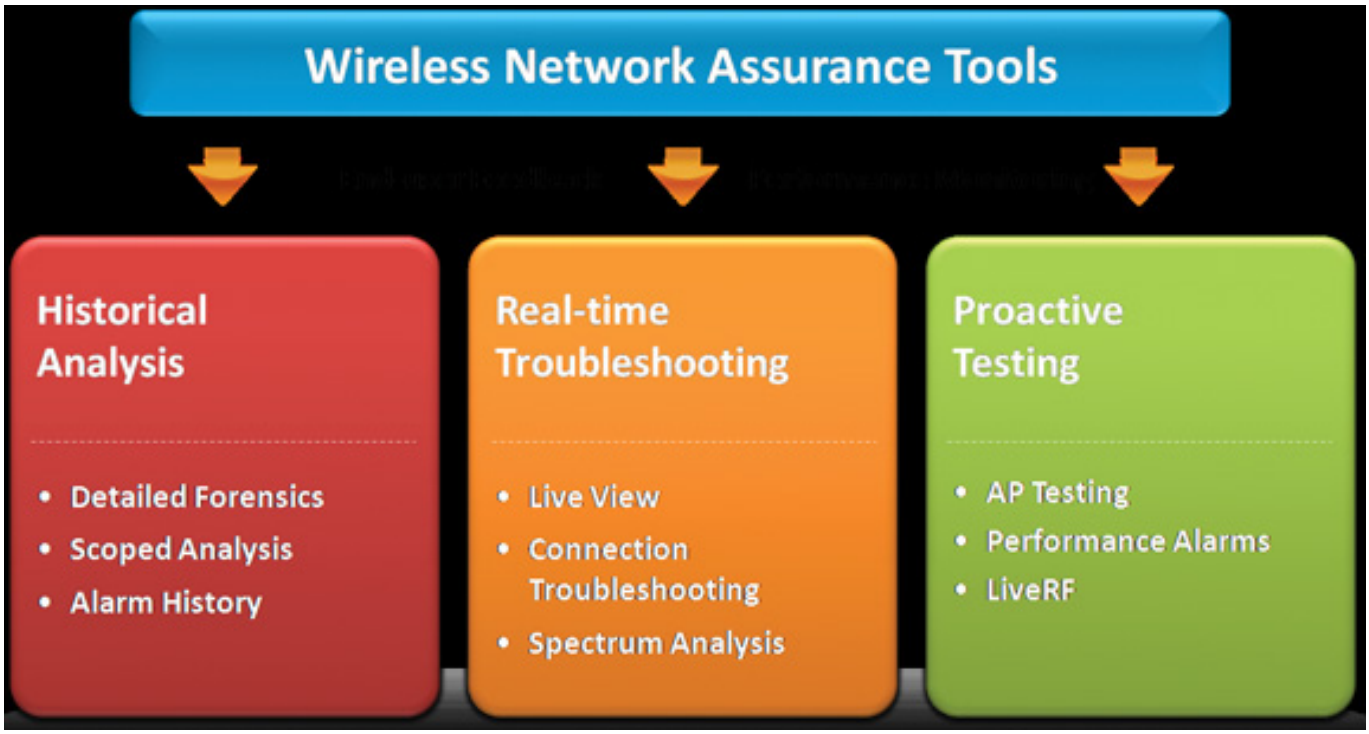
Connectivity Problems - Even with proper coverage and reduced interference levels, enterprise IT often gets support calls associated with wireless connectivity issues. For example, the WLAN network may be healthy but the user may have the wrong security settings, wireless interface hardware or driver issues, wireless supplicant issues or other problems that are preventing wireless access. Alternatively, the user's client might be ok but the AP might be misconfigured, damaged or may have a hardware problem. Sometimes a wireless connectivity problem may not even be a wireless layer issue – the problem may be on the wired side of the network, such as a DNS, DHCP or firewall problem.

Roaming Issues - Another common problem that affects mobile wireless clients is roaming. This particularly impacts Voice over WLAN clients that have stringent jitter and latency requirements. When a mobile client roams, it may have to change the AP it is connected to. Roaming across APs efficiently and securely is a challenging requirement. Troubleshooting roaming problems is even more challenging. A static connection between a client and a fixed AP can be analyzed with a laptop analyzer. However, a mobile client associating with several APs makes laptop-based analysis cumbersome.

Helpdesk-Optimized Wireless Network Assurance Tools

A holistic WLAN management platform should include a suite of network assurance tools for centralized WLAN support and troubleshooting – Historical Analysis tools to solve known and reported problems, Real-Time Troubleshooting tools to get an instant view of the WLAN, as well as Proactive Testing tools that check the network and identify future problems before they get flagged by users. Performance issues

can be user reported or self-diagnosed by the system through active monitoring.



Historical Analysis
Historical or forensic analysis tools allow administrators to analyze device specific trends over time to better understand the root cause of a problem or detect intermittent issues. Wireless events are, by their nature, transient. This presents an enormous problem for administrators researching complex and intermittent performance issues. The ability to rewind and review detailed records of wireless activity provides valuable historical insights into complex wireless performance issues. Some WLAN monitoring systems are capable of maintaining hundreds of minute-by-minute wireless device statistics such as channel utilization, signal and noise characteristics, device activity, association information and traffic flows. The historical data can be trended and analyzed over configurable time windows. The forensic data can also be leveraged effectively to automatically generate performance summary reports and have them sent to the wireless network administrator. Large deployments may have different individuals assigned to different geographies. The ability to scope-limit forensics and reporting to user defined portions of the network hierarchy is important for scalability.

Real-time Troubleshooting
Real-time wireless analysis tools allow the administrator to look into what is happening in the WLAN at the 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. WLAN monitoring systems can use 24x7 monitoring sensors to provide remote Layer 2 packet capture capabilities. A variety of analyses can be performed centrally based on data provided by remote sensors such as connection diagrams, traffic flow charts, capacity and channel utilization statistics. The sensor radio can also provide Layer 1 spectrum analysis capabilities allowing network administrators to identify and classify possible sources of interference such as microwave ovens, Bluetooth devices and frequency-hopping

phones. Embedding software-controlled spectrum analysis capabilities in sensor radios allows enterprises to perform on-demand as well as background interference detection across the entire deployment as opposed to selectively deploying expensive hardware-based analyzers in limited subset of locations.

Wireless client connectivity problems can be caused by a variety of issues, many of which are not even related to the wireless network. As the number of wireless users increases, escalating every wireless issue to experts is unsustainable. Remote wireless troubleshooting tools geared towards Tier-1 helpdesk personnel, with limited wireless networking expertise, are needed to facilitate remediation of wireless connectivity problems at remote locations. These tools should quickly identify device configuration problems, wireless network health, wireless network availability and wired network connectivity issues when a user calls the helpdesk.

Proactive Testing

As the WLAN scales, the ability to transform from a reactive to a proactive wireless support organization is important. Sensor-based automated remote AP testing solutions can check and validate the WLAN as seen from a wireless client's perspective. By utilizing the dedicated radio of a wireless sensor to simulate a wireless client station, true end-to-end network testing can verify all aspects of the wireless application's data path. Connectivity tests can be customized to verify the specific wireless configuration, wired network configuration and application availability. These tests can be configured to run automatically on a pre-defined schedule or on-demand as needed to proactively identify issues before they impact users.

Sensor-based monitoring tools can constantly measure and predict RF coverage across the enterprise's WLAN deployment, providing remote assessment and real-time visualization of the wireless network. Transient sources of interference, changing office layouts and physical obstructions require ongoing vigilance after a deployment to ensure the WLAN network is capable of supporting necessary wireless applications. Live RF monitoring addresses these challenges by collecting and analyzing the data gathered from the WLAN infrastructure to create real-time maps of RF signal propagation and application coverage. Background monitoring ensures coverage problems are detected prior to impacting end users. Side-by-Side comparisons of the live RF coverage with what was planned for can quickly pin-point areas of degraded performance before users start submitting those helpdesk tickets, enabling IT to proactively stay ahead and on top of any WLAN issues.