Centralized WLAN Troubleshooting in Healthcare

Maximizing Availability to Critical Wireless Applications

Centralized WLAN Troubleshooting

Wireless Local Area Networks (WLAN) have proliferated within healthcare environments. The staff efficiencies and patient care advantages realized through wireless mobility are well established. WLAN infrastructure solutions have matured, and provide reasonable interoperability under the Wi-Fi certification program. 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 critical healthcare applications migrate to wireless, the cost of troubleshooting and fixing wireless network connectivity and performance issues is increasing. Unlike wired networks, wireless networks pose unique challenges given the transient and shared nature of the communication medium. The ability to effectively analyze and respond to wireless problems is indispensable for maximizing the Return-on-Investment (ROI) from a WLAN solution. This paper provides a summary of some of the key wireless performance issues that affect WLAN deployments in healthcare. The paper also covers the components of the Motorola AirDefense Network Assurance suite, the vendor agnostic, WLAN troubleshooting solution that can significantly improve wireless network availability and therefore the performance of data, voice and other healthcare applications.

WLAN Performance Challenges in Healthcare

WLAN networks 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 often affecting WLAN performance are illustrated in Figure 1.
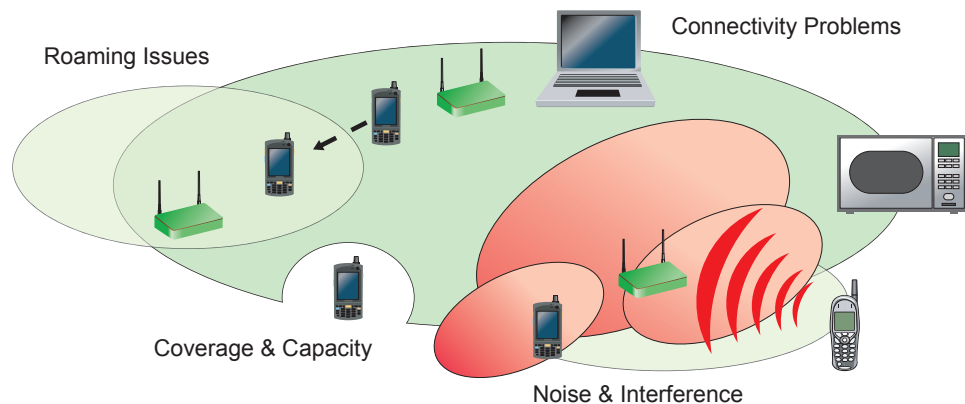

Figure 1: Common problems affecting WLAN performance

These problems tend to be overly pronounced in healthcare environments. This is due to the nature of wireless use in healthcare facilities, which includes the following characteristics:

- **Dynamic and Dense Environment:** The constant movement of people and equipment throughout healthcare environments, coupled with the ebb and flow of application usage at various times of the day and week, means that the RF profile can be unpredictable.
- **High Wall Density with Varying RF Attenuation:** Patient rooms with ceramic tile bathrooms, fire-stop walls, lead walls near radiology, and walls with med-gas lines dramatically attenuate wireless signals as do elevators, and exterior brick walls that become interior walls as new hospital wings are added. When dense wall construction is combined with long, unobstructed hallways, RF patterns can vary dramatically leading to coverage holes in some areas and too much signal (co-channel interference) in others.
- **Variety of RF devices:** Hospitals utilize a wide and ever-expanding variety of RF devices across the spectrum, including a fast-growing set of devices concurrently reliant upon 802.11. This often includes a mixture of point-of-care devices for data (laptops, Computers-on-Wheels, data collection devices, etc.), Voice-over-WLAN devices, medical equipment with built-in WLAN radios, and more.
- **Extremely mobile staff:** Nurses and other caregivers often spend the majority of a shift on

the move, and access mobile devices while moving, creating frequent roaming issues.

- **Critical applications:** Many of the applications running over wireless networks in healthcare environments are considered critical to a patient's safety, placing extra scrutiny on any delays, downtime or other issues.

Coverage and Capacity

WLANs typically consist of Access Points (APs) distributed across a facility or set of facilities. RF signal strength wanes as the distance from the transmitting source increases. Indoor RF propagation is strongly affected by scattering and multipath in the environment, which in turn depends on the obstacles and building characteristics. Careful site survey and planning is needed to optimize the placement of APs to assure robust coverage where needed. Despite best efforts, most healthcare deployments still suffer from coverage holes. Apart from zones where consistent signal fading occurs, there may still be areas where the practical wireless throughput is lower than expected. Being unable to connect to the wireless network or having a poor connection can be frustrating and result in reduced productivity.

Sometimes, despite good signal strength, users experience reduced throughput from the WLAN. This often happens when other users are consuming excessive shared bandwidth or when the AP is overloaded. One slow connection can bring down the whole network. This often happens when a user on the periphery of an AP's coverage (operating at lower data rates) is utilizing the network excessively. Since WLANs use a fair channel sharing algorithm, the slow user gets to access the channel as frequently as the fast user. The situation is similar to a fast car being stuck behind a slow truck on a single lane highway. Another common performance bottleneck is excessive clients connected to a single AP.

Noise and Interference

The RF medium used by WLANs has ambient thermal noise as well as interference introduced by other devices radiating energy in the same frequencies used by the WLAN. 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. Excessive noise and interference will increase the packet error rate in the WLAN leading to reduced wireless throughput and potential loss of connectivity.

Since RF interference is hard to "see" and quantify without sophisticated spectrum analyzers and other costly RF equipment, IT is often left guessing at what the potential source of wireless performance degradation might be. Many interference sources are transient and only detected intermittently, exacerbating the complexity of wireless troubleshooting. For example, a microwave oven in the office might be on during lunch break, seriously degrading the WLAN in its vicinity during mid-day.

Co-channel interference is another common problem for WLANs. Since APs often limit coverage to provide wireless access over a large area, a frequency reuse pattern can be used to allow two adjacent APs to operate without collisions. The number of non-overlapping channels in the 2.4 GHz band is limited to three. This forces enterprises to re-use the same frequencies across the deployment. This creates co-channel interference where two APs and their associated devices are operating on one channel causing increased collisions resulting in higher packet error rates.

Connectivity Problems

Even with proper coverage and reduced interference levels, IT departments often receive support calls associated with wireless connectivity issues. For example, the WLAN could be healthy but a user may have a wrong security key, a bad wireless driver, wireless supplicant issues or other tools preventing wireless connections. Alternatively, the user's client might be fine, but the AP could be misconfigured, an antenna might have fallen off or the AP may have a hardware problem. Sometimes a wireless connectivity problem may not even be a wireless access issue – the problem may be on the wired side of the network (a bad gateway for example). Having to rule out coverage, capacity, noise and interference problems is daunting enough, not to mention user error, device/software misconfigurations and wired network issues.

Roaming Issues

Another common problem affecting mobile wireless clients is roaming. This particularly impacts Voice over WLAN (VoWLAN) clients with stringent jitter and latency requirements. When a mobile client roams, it may have to switch its AP connection. Roaming between APs efficiently and securely is a challenging requirement, and an especially common complaint within healthcare environments. 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. A distributed monitoring system can automatically lock onto a mobile client and provide a centralized, consolidated view of its behavior as the client roams, significantly simplifying troubleshooting.

Centralized WLAN Troubleshooting

The operational cost of a WLAN increases significantly as performance problems increase. 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, healthcare IT often struggles with effective resolution of wireless network problems. When a user calls a help desk complaining about the lack of wireless connectivity, the inability of the support staff to immediately look at the RF medium and analyze wireless traffic around the user often results in inadequate problem resolution or necessitates the presence of a field technician with a laptop wireless analyzer to further investigate the problem. This method leads to increased cost and longer resolution times for wireless trouble tickets, not to mention decreased productivity in the interim. Often, when a field technician shows up on site, the problem might not even manifest itself, especially if the root cause is a transient noise source. 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 AirDefense Network Assurance suite runs on the AirDefense Services Platform, the industry's first comprehensive service oriented platform that can be leveraged by enterprise IT to dramatically reduce the TCO and achieve quicker ROI from their WLAN. Figure 2 illustrates the AirDefense Network Assurance solution and summarizes the WLAN troubleshooting tools.

The system uses a network of Access Points (APs) or dedicated RF sensors that continuously monitor the airwaves – intelligently scanning different frequencies over time and space to detect WLAN performance problems and policy violations. The remote APs or sensors serve as the "eyes and ears" of the WLAN, observing network behavior 24x7 and allowing administrators to "look into" a wireless issue from any location with network access. APs with special firmware allowing "promiscuous mode" packet visibility are used as dedicated sensors. Promiscuous mode allows sensors to listen to all the packets received by an antenna.

The sensors use an intelligent channel scanning algorithm to detect WLAN traffic and interference sources across the RF spectrum. The sensors locally analyze the received packets, collect several statistics and events of interest and use an efficient Application Programming Interface (API) to communicate over a secure link to the centralized appliance. Sensor software can be enabled on dedicated radios available in the Motorola WLAN infrastructure – a dual-radio Motorola AP can have AP functions enabled on one radio and 24x7 sensing enabled on the second radio. Alternatively, sensor only functions can be enabled on a dedicated device and the system can be overlaid on any WLAN infrastructure to provide vendor agnostic WLAN performance monitoring and troubleshooting.

The appliance correlates events and statistics from the sensors and provides a centralized data repository. The appliance also allows the system to be administered and managed from one point. Performance policies can be specified on the appliance and various WLAN performance reports can be automatically generated and archived by the appliance.

Motorola AirDefense Solutions
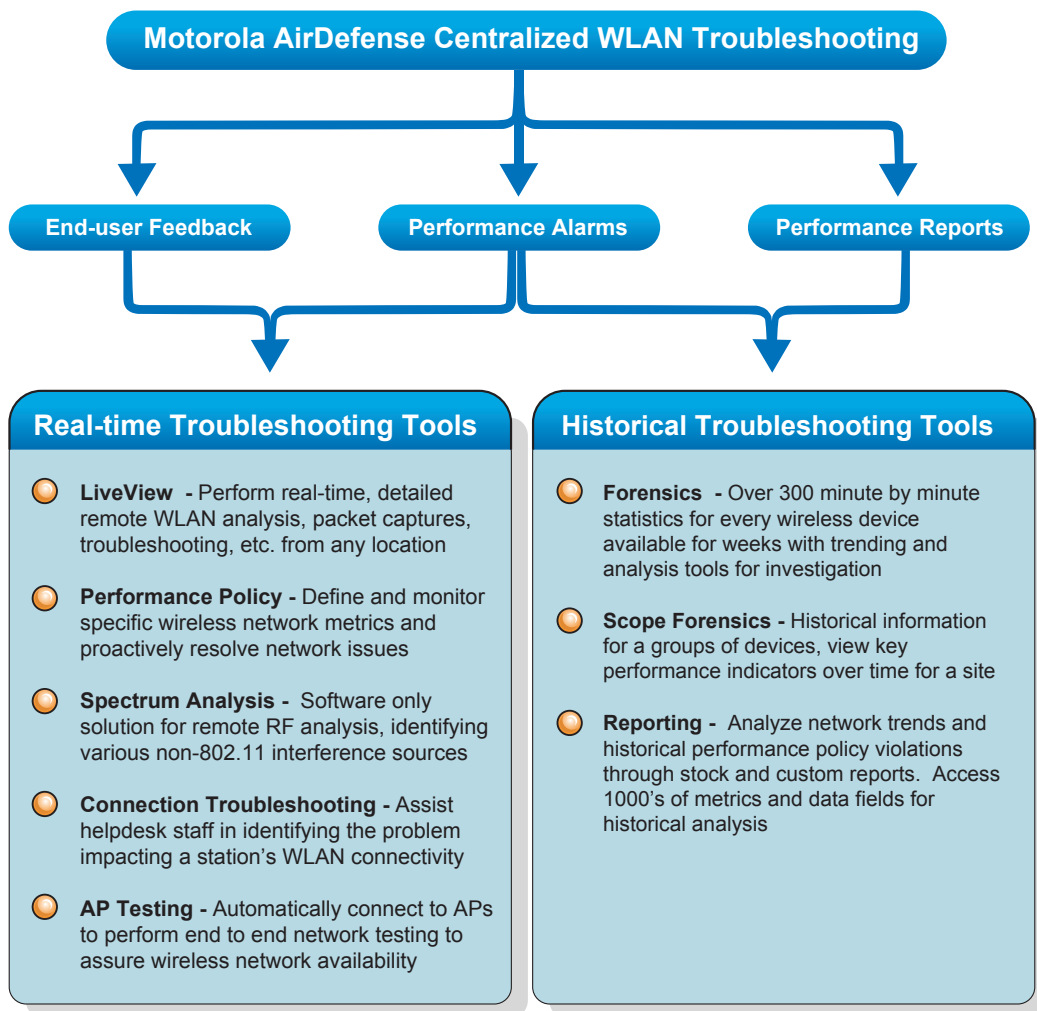
Centralized Wireless Monitoring

Motorola AirDefense Centralized WLAN Troubleshooting

End-user Feedback   **Performance Alarms**   **Performance Reports**

Real-time Troubleshooting Tools

- **LiveView** - Perform real-time, detailed remote WLAN analysis, packet captures, troubleshooting, etc. from any location

- **Performance Policy -** Define and monitor specific wireless network metrics and proactively resolve network issues

- **Spectrum Analysis -** Software only solution for remote RF analysis, identifying various non-802.11 interference sources

- **Connection Troubleshooting -** Assist helpdesk staff in identifying the problem impacting a station's WLAN connectivity

- **AP Testing -** Automatically connect to APs to perform end to end network testing to assure wireless network availability

Historical Troubleshooting Tools

- **Forensics -** Over 300 minute by minute statistics for every wireless device available for weeks with trending and analysis tools for investigation

- **Scope Forensics -** Historical information for a groups of devices, view key performance indicators over time for a site

- **Reporting -** Analyze network trends and historical performance policy violations through stock and custom reports. Access 1000's of metrics and data fields for historical analysis
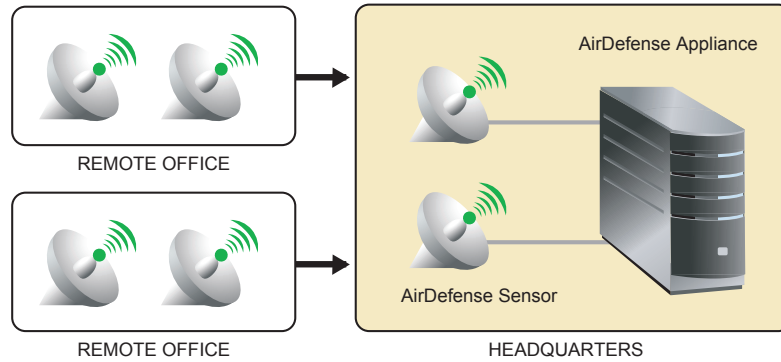
Figure 2: Centralized WLAN troubleshooting using the AirDefense Network Assurance Solution

Performance problems are flagged in three ways.

1. **End-user feedback:**
   A WLAN user can call an IT helpdesk reporting a wireless problem. A ticketing system can issue a trouble ticket and forward the problem to the wireless IT support staff.

2. **System performance alarms:**
   The system has various performance monitoring alarms built in. If enabled, the system can detect congestion, noise, interference sources, coverage and capacity issues and generate an alarm. The alarm can be viewed on the system console, sent as an email to an administrator or forwarded to a Network Operations Center (NOC) using standard protocols (such as SNMP traps or SYSLOG).

3. **System performance reports:**
   Various performance thresholds and criteria can be specified in the system. The system audits the WLAN 24x7 based on the specified criteria and generates reports automatically. The report can point to systematic problems detected on the WLAN over time.

Once a problem is flagged, the system provides sophisticated real-time and historical troubleshooting tools.

Real-time Troubleshooting Tools

Real-time tools allows an administrator to look into what is happening on 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.

Client Connectivity Troubleshooting

Client connectivity problems can be caused by a variety of issues, many of which are not related to the wireless network. Unfortunately, the wireless network often gets faulted for connectivity problems experienced by mobile users. The wireless network support staff is then required to devote time trouble-shooting issues which may not be a wireless problem. The AirDefense Client Connectivity Troubleshooting Wizard is designed to assist Tier-1 helpdesk personnel, with limited wireless networking expertise, to easily identify a connectivity problem. This allows them to either resolve it or escalate it to the appropriate IT support staff. The Client Connectivity Troubleshooting Wizard's sophisticated analysis engine quickly identifies device level problems, wireless network health, wireless network availability, wireless network or client configuration and wired network connectivity issues.
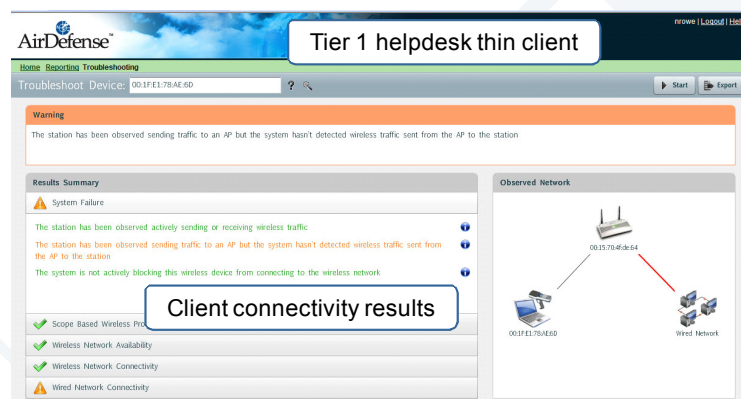

Figure 3: Wireless connection troubleshooting tool

The tool allows helpdesk staff to log onto a thin user interface with limited access to the AirDefense appliance. Using a device selection wizard, the helpdesk staff can remotely identify the wireless device via its hardware MAC address. The system then runs a series of connection tests enumerating success, failure or warning results for each step (as depicted in Figure 3). The system can present the analysis in simple terms, for example "the wireless network around the station is healthy" or "the station has been observed actively sending or receiving wireless traffic". This enables diagnosis and resolution of common wireless problems. Apart from troubleshooting a specific device, the tool also allows helpdesk personnel to employ a scope based analysis to analyze problems that might be affecting a group of devices.

Access Point (AP) Connectivity Testing

Wireless applications rely on the configuration of both wireless and wired network elements to function correctly. A simple change to the wired network could render wireless applications inoperable. Trouble-shooting can be cumbersome and time-consuming since network administrators cannot connect to the wireless network to perform the tests required to identify where the problem occurred. The AirDefense AP Connectivity Testing Module addresses these issues by allowing the remote testing of network connectivity from the perspective of a wireless station. By utilizing the radio of the wireless sensor to simulate a wireless client station, true end-to-end network testing can verify all aspects of the wireless application's datapath. Connectivity tests can be customized to verify the specific wireless configuration, wired network configuration and application server availability. These tests can be configured to run automatically on a pre-configured schedule (or on demand as needed) to proactively identify and notify configuration changes which impact wireless applications.
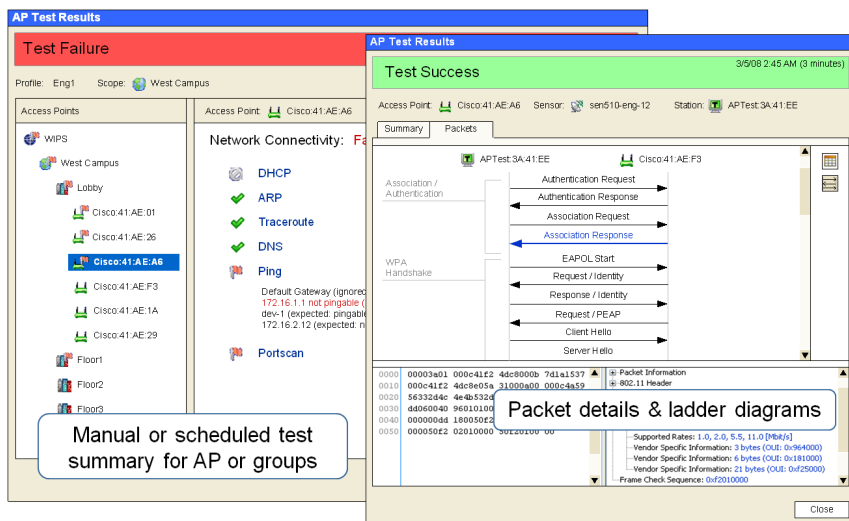

Figure 4: Access Point test results

Once an AP is chosen for testing, configuration data such as security keys, SSID, IP address settings is obtained via a user input or a pre-configured profile from the appliance. A sensor is chosen for the test. This is typically the sensor closest to the AP with the best received signal strength. Other sensors in range can also be used. The sensor is then locked on the AP's operating channel and several Layer 2 wireless tests and Layer 3 wired network tests are performed, as shown in Figure 4. If the AP uses 802.11i based security, a 4-way handshake is performed and temporal as well as group keys are installed. Based on the success of the Layer 2 connection, an appropriate report is generated. Once a successful Layer 2 connection is established, the sensor client tries to establish a Layer 3 session. If the sensor is configured for DHCP, it tries to automatically obtain an IP address, otherwise it uses pre-specified IP address settings. Once an IP address is obtained, the sensor performs a ping and traceroute test to determine if a client can successfully ping a known machine on the wired network.

Spectrum Analysis

The AirDefense Spectrum Analysis Module, the industry's first software only solution, can remotely view the physical layer of an enterprise WLAN using distributed sensors without requiring any additional specialized hardware. With the Spectrum Analysis Module, network administrators can identify and classify possible sources of interference in the 2.4 and 5 GHz WLAN frequency bands. Sources of interference could include microwave ovens, Bluetooth devices, frequency hopping phones and wireless cameras. Using the spectrum analysis tool, you can view the impact of WLAN interference sources without sending a technician with expensive hardware to a remote location.
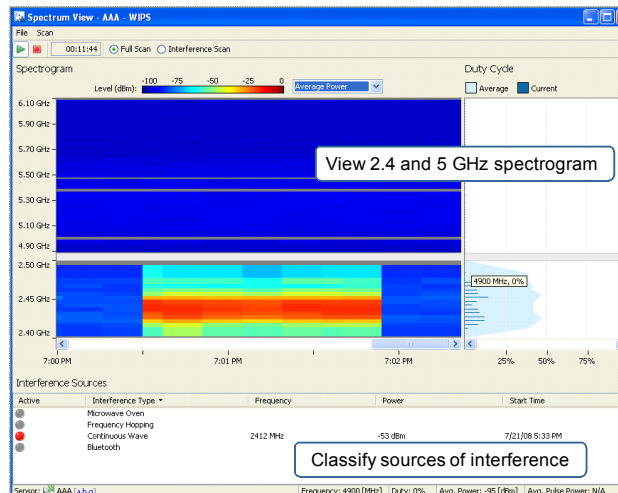
Figure 5: Spectrum analysis module showing spectrograms and interference classification

The Spectrum Analysis Module can work silently in the background, periodically scanning WLAN bands for sources of interference. If interference is detected, performance alarms are generated. In addition to background scanning, the spectrum analysis tool can be used in real-time to remotely analyze the WLAN spectrum at any deployed location. The tool plots a spectrogram in the 2.4 and 5 GHz bands and reports the observed power level in a given time-frequency bin (as depicted in Figure 5). Spectrograms are routinely used to analyze the wireless spectrum and determine how much energy is present on a given radio frequency at any instant. Wireless devices using different physical layer protocols often have unique spectral signatures that can be used to identify them.

LiveRF

The AirDefense LiveRF Module provides a remote assessment of network coverage and real time visualization of the wireless network. Transient sources of interference, changing utilization, and physical obstructions require ongoing vigilance after a deployment to ensure the WLAN network is capable of supporting necessary wireless applications. LiveRF 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. Real-time visualizations provide the data to streamline troubleshooting to solve problems faster. LiveRF equips administrators with the tools to operate and ensure a more reliable wireless network.

Performance Policy

The AirDefense Network Assurance suite proactively monitors the WLAN using a specified performance policy based on various metrics and thresholds. The system can be tuned to monitor for 50 device specific parameters, 7 environmental parameters and 50 performance specific events. The system can proactively identify and flag common wireless issues such as excessive utilization, interference sources, congestion and coverage issues, even before users experience a significant disruption.
Some of the performance alarms the system is capable of generating are as follows:

1. **Utilization Alarms:** The system has 33 utilization specific alarms that trigger when management, control and data frames of different types exceed a specified threshold. For example, the system can detect when the total number of associations in a Basic Service Set (BSS) has exceeded threshold, indicating an overloaded WLAN. Similarly, the system can detect when there are an excessive number of WLAN disassociations, indicating an overload or a potential denial of service attack.

2. **Congestion Alarms:** The system has 6 congestion alarms that can detect issues such as high channel noise levels and excessive station roaming.

3. **Coverage Alarms:** The system has 4 coverage specific alarms that can detect issues such as an AP communicating excessively using low data rates and hidden stations.

4. **Interference Alarms:** The system has 7 interference alarms capable of detecting common sources of interference such as microwave ovens, Bluetooth devices, continuous wave transmitters and frequency hopping phones. It can also detect non-standards based WLAN equipment (Atheros 'Turbo' mode devices, pre-standard 802.11n devices, etc.)

5. **Configuration/Compatibility Alarms:** The system has 8 configuration related alarms that can detect legacy mode transmissions that could be degrading network throughput and creating data rate mismatches between an AP and a station.

LiveView

The AirDefense LiveView function allows administrators to capture and analyze 802.11 packets from any location. Traditionally this feature was limited to laptop based analysis tools equipped with a WLAN card and special software to capture and analyze 802.11 frames. This limited approach used by other vendors, meant that the laptop along with the technician had to be physically present at the site where the problem had occurred. Our LiveView feature allows administrators to leverage the remote sensors to capture 802.11 packets and analyze them from any location. LiveView automatically uses distributed sensors to effectively capture frames from a device, removing duplicates and switching sensors as the device roams. A complete 802.11 packet analyzer is included within LiveView as depicted in Figure 6.
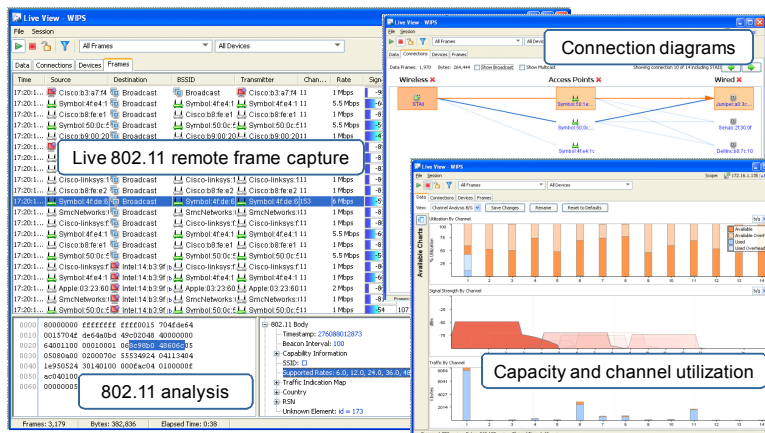

Figure 6: LiveView features

LiveView also allows the IT staff to analyze connection diagrams that establish the network link from a wireless device to an AP and all the way through to a wired device. Connection diagrams facilitate the visual analysis of device roaming behavior and traffic flow. LiveView supports 28 different analysis charts and allows the user to create customized views for individual devices as well as groups of devices based on different locations or scope. Capacity and channel utilization graphs can be generated in real-time providing valuable insights into performance bottlenecks as depicted in Figure 6.

Historical Troubleshooting Tools

Historical troubleshooting tools allow an administrator to analyze device specific trends over time to better understand the root cause of a problem or detect intermittent problems.

Advanced Forensics

Wireless events are by their nature transient. This presents an enormous problem for administrators researching complex and intermittent performance issues. Without granular historical activity records, research is virtually impossible. The AirDefense Advanced Forensics Module provides administrators the ability to rewind and review detailed records of wireless activity. This provides valuable historical insights into complex wireless performance issues.
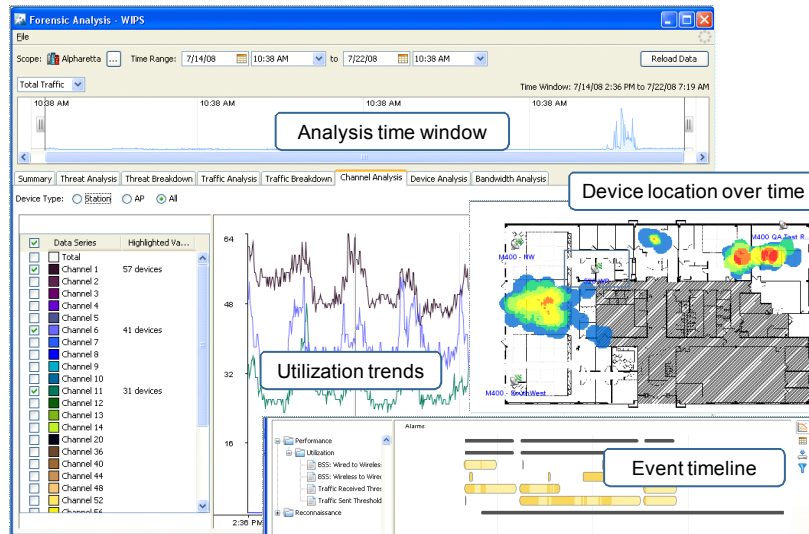
Figure 7: Historical performance analysis using the advanced forensics module

Administrators can view the activity of a poorly performing device over a period of months and drill down to minute-by-minute wireless activity. The system maintains 325 data points per minute for every wireless device. Statistics stored by the system include critical device communication and traffic information, channel utilization, signal and noise characteristics, device activity and traffic flow. This historical data can be trended and analyzed over configurable time windows. The system can re-create a timeline and sequence of events identifying specific instances when performance problems occurred (as depicted in Figure 7). Historical association analysis can show how clients have been connecting to APs in the past and identify imbalances, such as over or under utilized APs. Historical traffic analysis can quickly isolate anomalous behaviors, such as a device suddenly sending excessive traffic or periodic problems such as connectivity loss when a microwave oven is operating in the vicinity of an AP (at lunch time). Historical channel analysis can determine spare channel capacity and help optimize WLAN frequency planning. Historical location tracking can determine the physical location of a device over time, identifying hot zones where the device typically operates, and roaming trajectories for mobile clients.

Performance Reports
Advanced forensics provides an interactive tool for historical performance analysis. While an interactive tool is needed for troubleshooting complex and intermittent problems, often the ability to automatically generate performance summary reports based on historical data and have it automatically sent to wireless network administrators is desirable. Network Administrators can schedule and automatically generate granular performance reports through the AirDefense Services Platform. Fully customizable reports can be generated in a variety of formats such as HTML, CSV and PDF. Key performance indicator reports can be automatically sent to IT executives to validate the benefits of WLAN mobility and quantify ROI. Detailed reports delivered to the network administrators can help them track performance and identify potential problems ahead of time.

Conclusions

Managing large distributed WLANs within the difficult environment of healthcare poses unique challenges. Unlike wired networks, WLANs have to operate in a shared wireless medium that is constantly changing. WLAN performance and coverage can be significantly impacted by noise and transient interference in the local air space. Wireless devices are mobile and frequently roam between different WLANs. Mobile devices often have incorrect settings preventing a device from successfully communicating. The cost of trouble-shooting wireless problems is significant. Typically, when a user reports connectivity problems, an on-site technician armed with a wireless laptop based network analyzer is sent on site to capture wireless traffic and analyze the root cause of the issue. This method is costly and time consuming. The ability to "look into" a wireless network remotely from a central facility is indispensable for efficient WLAN troubleshooting.

The AirDefense Network Assurance suite offers a unique set of tools for vendor agnostic, remote WLAN performance management and troubleshooting. The system features powerful real-time tools to capture and analyze 802.11 frames, detect and classify non-802.11 sources of interference, monitor performance policy violations and remotely debug client and AP connectivity issues. The system also maintains minute-by-minute granular information for all monitored devices and facilitates reporting and historical troubleshooting of complex and intermittent problems. The solution proactively optimizes wireless LAN performance as well as ensure network reliability and offers unmatched remote troubleshooting and network monitoring capabilities. The net result is that healthcare organizations can maximize the availability of their WLAN while simultaneously reducing operational expenses.

MOTOROLA