



ENTERPRISE & MOBILITY

Centralized WLAN Troubleshooting in Healthcare

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. This document examines how to maximize availability to critical wireless applications.

BROCADE

CENTRALIZED WLAN TROUBLESHOOTING

Wireless Local Area Networks (WLANs) 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 they 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 document provides a summary of some of the key wireless performance issues that affect WLAN deployments in healthcare. The document also covers the components of the AirDefense® Enterprise Appliances for Brocade® Mobility, the vendor-agnostic, WLAN troubleshooting solution that significantly improves wireless network availability and, therefore, improves 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 that often affect WLAN performance are illustrated in Figure 1.

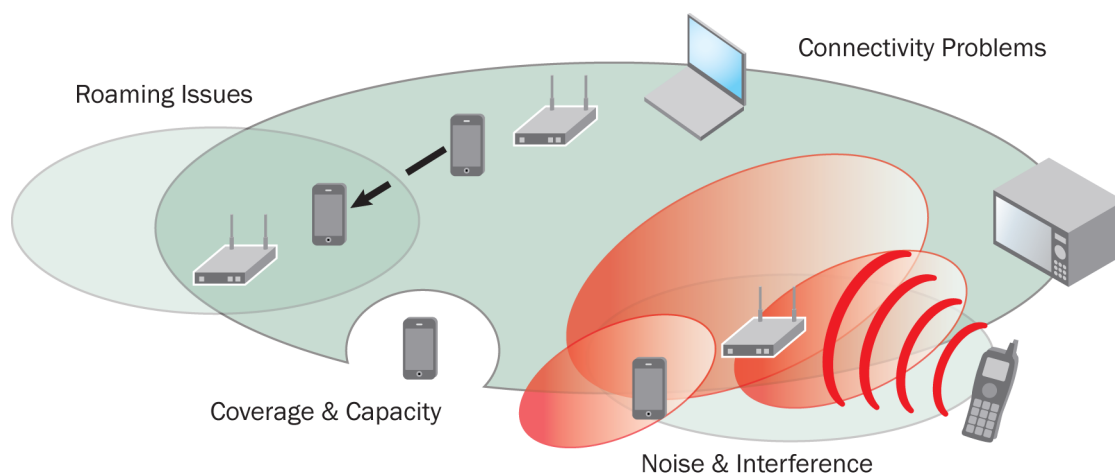


Figure 1. Common problems affecting WLAN performance

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 on IEEE 802.11. This often includes a mixture of point-of-care devices for data (such as laptops, Computers-on-Wheels, data

collection devices, and so on), Voice over WLAN (VoWLAN) 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, accessing mobile devices while moving, which frequently creates roaming issues.
- **Critical applications:** Many of the applications running over wireless networks in healthcare environments are considered critical to patient safety, which places extra scrutiny on delays, downtime, or other issues.

Coverage and Capacity

WLANs typically consist of Access Points (APs) that are 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 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 can 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 is allowed 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 caused when an excessive number of clients is 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 that radiate energy in the same frequencies used by the WLAN. WLANs operate in the Industrial, Medical, and Scientific (ISM) license-free bands (2.4 GHz and 5 GHz) that are shared by other wireless protocols and devices such as Bluetooth, cordless phones, microwave ovens, wireless cameras, and so forth. Excessive noise and interference increases 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 staff are often left to guess at what the potential source of wireless performance degradation might be. Many interference sources are transient and can be detected only intermittently, exacerbating the complexity of wireless troubleshooting. For example, a microwave oven being used in an office during lunch break, might seriously degrade the WLAN in its vicinity during midday.

Co-channel interference is another common problem for WLANs. Since APs often limit coverage, in order 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 reuse 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 and 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, even if the WLAN is healthy, a user might 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 operating properly, but the AP might be misconfigured, an antenna might have fallen off, or the AP might have a hardware problem. Sometimes a wireless connectivity problem might not even be a wireless access

issue—instead, the problem might be on the wired side of the network (a bad gateway, for example). It is daunting enough to attempt to rule out coverage, capacity, noise, and interference problems, much less user error, device or software misconfigurations, and wired network issues.

Roaming Issues

Another common problem affecting mobile wireless clients is roaming. This particularly impacts VoWLAN clients with stringent jitter and latency requirements. When a mobile client roams, it might 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 poses an even greater challenge. 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, which significantly simplifies the troubleshooting process.

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. It can even necessitate further investigation of the problem by a field technician with a laptop wireless analyzer. This method leads to increased cost and longer resolution times for wireless trouble tickets, not to mention decreased productivity while waiting for problem resolution. Often, the problem does not even manifest at the same time that a field technician is present on site to investigate, especially if the root cause is a transient noise source. This makes identifying a solution very difficult. Thus, the ability to remotely troubleshoot and resolve WLAN performance problems in real time, with access to historical data to provide perspective, is crucial for maximizing availability and ROI from a WLAN.

AirDefense Enterprise Appliances for Brocade Mobility solutions provide the industry's most powerful wireless Intrusion Prevention System (IPS). The AirDefense Enterprise Appliances for Brocade Mobility solutions include several innovative and separately licensable add-on software modules that augment the appliances' base capabilities. Figure 2 summarizes the WLAN troubleshooting tools.

The system uses a network of 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 24 x 7 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 **AirDefense Enterprise Appliances for Brocade Mobility**. Sensor software can be enabled on dedicated radios available in the Brocade Mobility WLAN solutions: A dual-radio Brocade Mobility Access Point can have AP functions enabled on one radio and 24 x 7 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 **AirDefense Enterprise Appliances for Brocade Mobility** correlate events and statistics from the sensors and provides a centralized data repository. The appliances also allow 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.

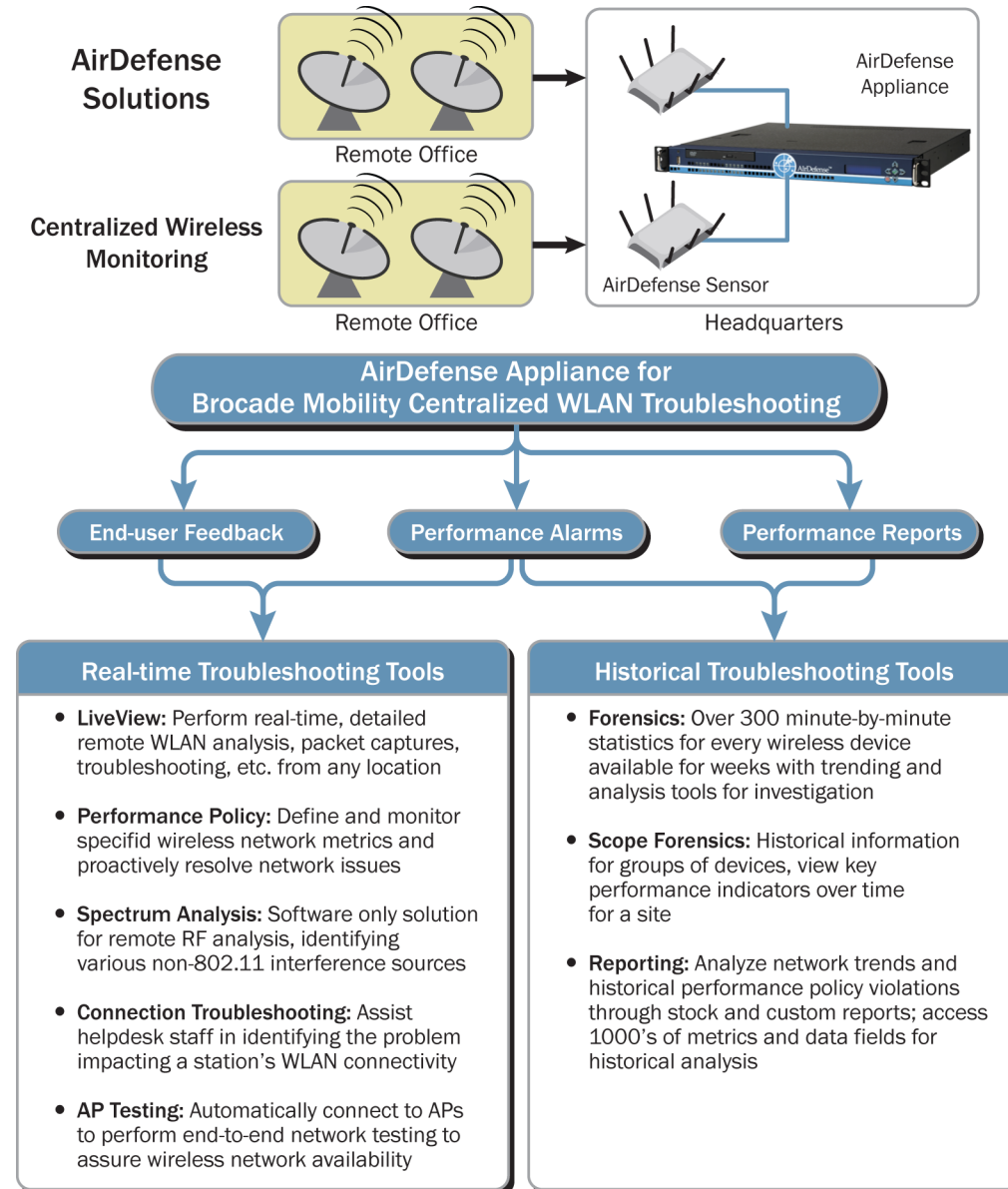


Figure 2. Centralized WLAN troubleshooting using the AirDefense Enterprise Appliances for Brocade Mobility solutions

Performance problems are flagged in three ways.

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

System performance alarms: The system has various performance monitoring alarms built in. If enabled, the system can detect congestion, noise, interference sources, and coverage and capacity issues and can 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 Simple Network Management Protocol [SNMP] traps or SYSLOG).

System performance reports: Various performance thresholds and criteria can be specified in the system. The system audits the WLAN 24 x 7, 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 allow an administrator to look into what is happening on the WLAN at a given instant. Many RF issues are hard to replicate or are 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 is mistakenly assigned fault for connectivity problems experienced by mobile users. The wireless network support staff is then required to devote time troubleshooting and issue that may not even be a problem with the wireless. The AirDefense Client Connectivity Troubleshooting Wizard is designed to assist Tier 1 helpdesk personnel, who might have 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 sophisticated analysis engine of the AirDefense Client Connectivity Troubleshooting Wizard quickly identifies device-level problems, wireless network health, wireless network availability, wireless network or client configuration, and wired network connectivity issues.

The screenshot displays the AirDefense Client Connectivity Troubleshooting Wizard interface. At the top, the AirDefense logo is visible. Below the logo, there is a navigation bar with 'Home', 'Reporting', and 'Troubleshooting' options. A search bar labeled 'Troubleshoot Device:' contains the MAC address '00:1F:E1:78:AE:6D'. To the right of the search bar are 'Start' and 'Export' buttons. Below the search bar is a warning message: 'Warning: The station has been observed sending traffic to an AP but the system hasn't detected wireless traffic sent from the AP to the station'. The main content area is divided into two sections: 'Results Summary' and 'Observed Network'. The 'Results Summary' section contains a table with the following entries:

| Results Summary | |
|--|------------------|
| System Failure | |
| The station has been observed actively sending or receiving wireless traffic | Information icon |
| The station has been observed sending traffic to an AP but the system hasn't detected wireless traffic sent from the AP to the station | Information icon |
| The system is not actively blocking this wireless device from connecting to the wireless network | Information icon |
| Scope Based Wireless Problems | Checkmark icon |
| Wireless Network Availability | Checkmark icon |
| Wireless Network Connectivity | Checkmark icon |
| Wired Network Connectivity | Warning icon |

The 'Observed Network' section shows a diagram of the network topology. It features a central wireless router with MAC address '00:15:70:4f:de:64'. A laptop with MAC address '00:1F:E1:78:AE:6D' is connected to the router via a black line. A 'Wired Network' is also connected to the router via a red line.

Figure 3. AirDefense Client Connectivity Troubleshooting Wizard

The wizard allows helpdesk staff to log onto a thin user interface with limited access to the **AirDefense Enterprise Appliances for Brocade Mobility**. 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. Troubleshooting 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 data path. 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 preconfigured schedule (or on demand as needed) to proactively identify and notify configuration changes that impact wireless applications.

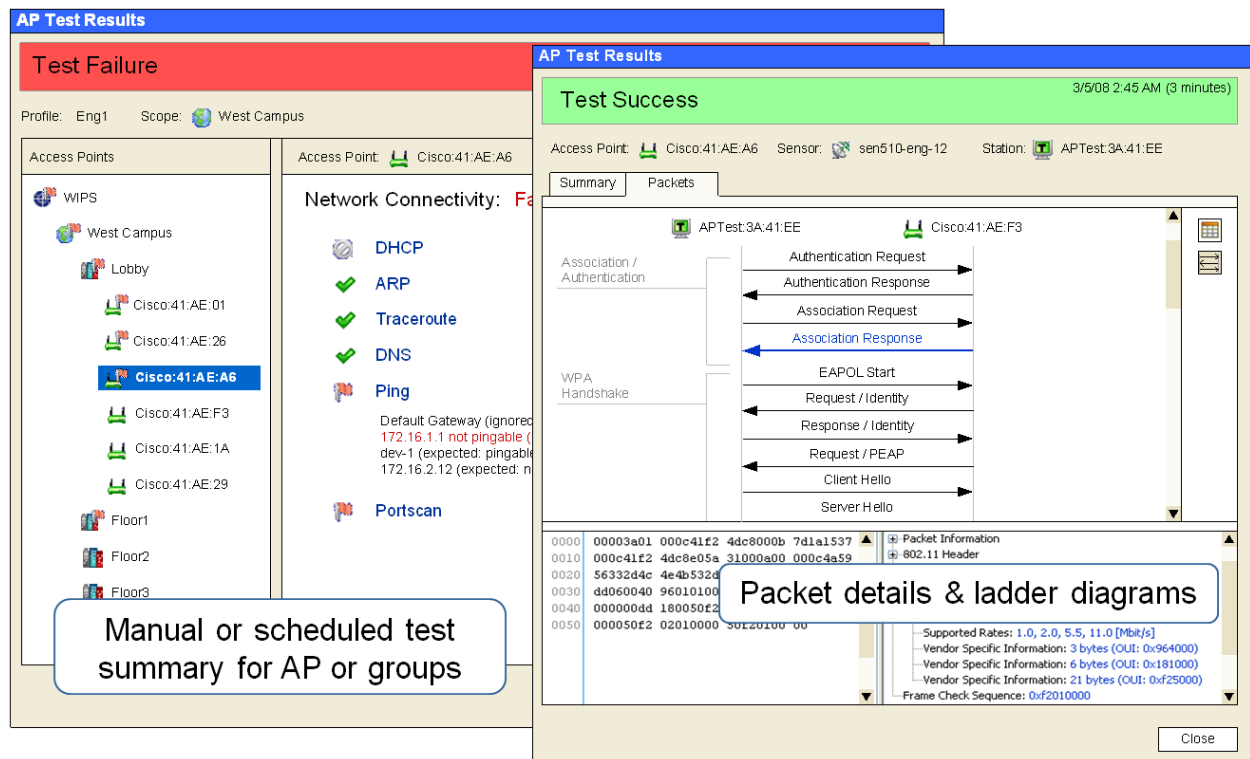


Figure 4. Access point test results

Once an AP is chosen for testing, configuration data such as security keys, Service Set Identifier (SSID), and IP address settings is obtained from the appliance via a user input or a preconfigured profile. A sensor is chosen for the test. This is typically the sensor closest to the AP with the best-received signal strength. Other sensors that are in range can also be used. The sensor is then locked on the operating channel of the AP, 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 prespecified 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 AirDefense 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 might 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.

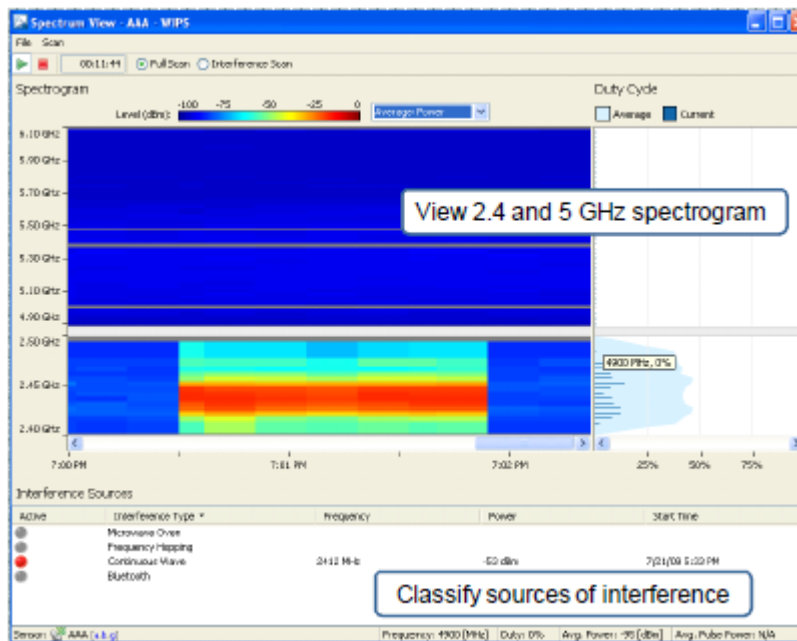


Figure 5. AirDefense Spectrum Analysis Module spectrograms and interference classification results

The AirDefense 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 that coverage problems are detected prior to impacting end users. Real-time visualizations provide the data to streamline troubleshooting and 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, and congestion and coverage issues, even before users experience a significant disruption.

These are some of the performance alarms that the system is capable of generating:

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.

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

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

Interference Alarms: The system has seven interference alarms that are 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 (such as Atheros Turbo mode devices, prestandard 802.11n devices, and so forth).

Configuration/Compatibility Alarms: The system has eight 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. The AirDefense 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.

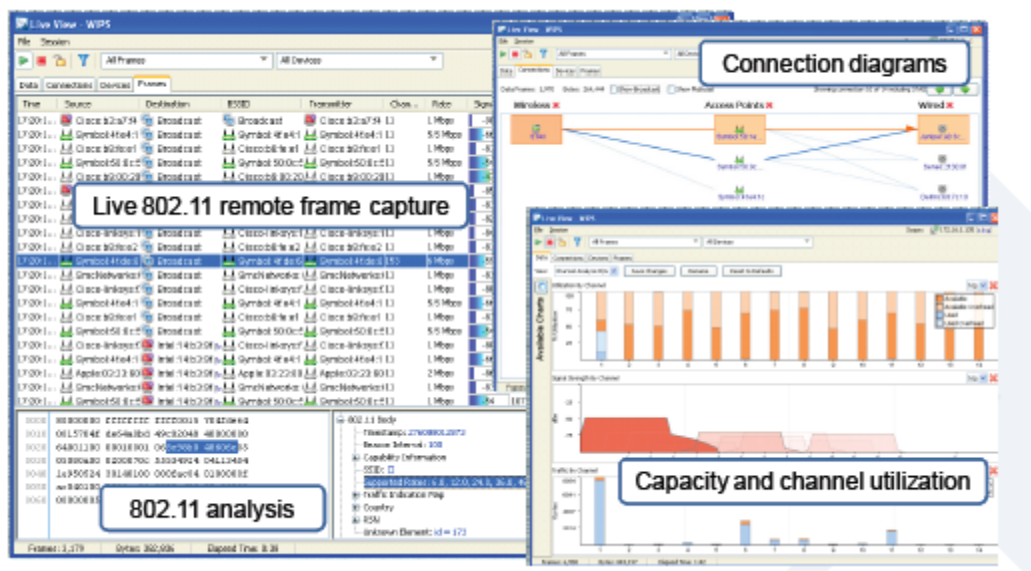


Figure 6. AirDefense LiveView results

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 who are 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 offers valuable historical insights into complex wireless performance issues.

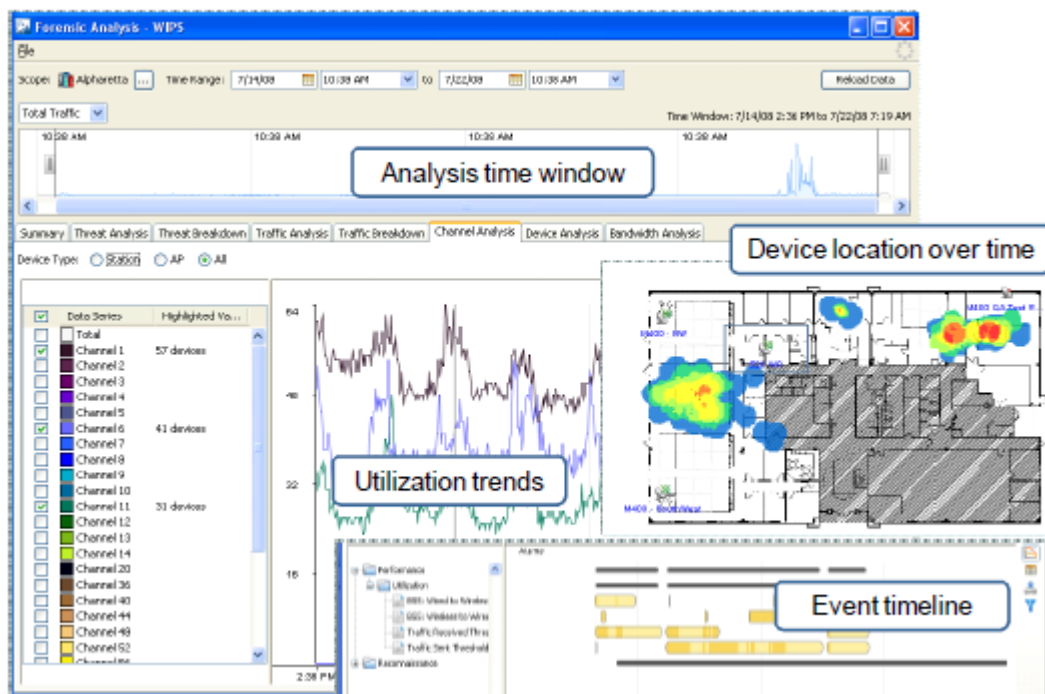


Figure 7. Historical performance analysis using the AirDefense Advanced Forensics module

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 connected to APs in the past and can identify imbalances, such as over- or underutilized 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. 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

The AirDefense Advanced Forensics Module provides an interactive tool for historical performance analysis. While an interactive tool is needed for troubleshooting complex and intermittent problems, often it is desirable to be able to automatically generate performance summary reports based on historical data and have it automatically sent to wireless network administrators. 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 before they occur.

BROCADE MOBILITY WLAN SOLUTIONS

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 they frequently roam between different WLANs. Mobile devices often have incorrect settings that prevent a device from successfully communicating. The cost of troubleshooting wireless problems is significant. Typically, when a user reports connectivity problems, a 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 Appliances for Brocade Mobility offer a unique set of tools for vendor-agnostic, remote WLAN performance management and troubleshooting. Three appliance models are available:

- **AirDefense 1252 Appliance for Brocade Mobility:** Packaged in a rack-optimized 1U chassis, the AirDefense 1250 provides 250 GB of storage for small WLAN deployments. It accommodates an Intel Pentium 4 3.4-GHz Processor and 1 GB of Error-Correcting Code DDR2 memory support.
- **AirDefense 3652 Appliance for Brocade Mobility:** Packaged in a rack-optimized 1U chassis, the AirDefense 3650 provides 250 GB of storage in RAID 1 configurations for medium-size to large WLAN deployments. It accommodates an Intel Core Duo 2.13-GHz Processor and 4 GB of Error-Correcting Code DDR2 memory support.
- **AirDefense 4250 Appliance for Brocade Mobility:** Packaged in a 2U chassis, the AirDefense 4250 provides 500 GB of storage in RAID 1 configurations and a redundant power supply for large to very large WLAN deployments. It accommodates an Intel 2.33-GHz Xeon 5140 Dual-Core Processor and 8 GB of fully buffered DDR2 memory support.

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 solutions proactively optimize WLAN performance, as well as ensuring network reliability and offering 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.

© 2011 Brocade Communications Systems, Inc. All Rights Reserved. 11/11 GA-TB-417-00

Brocade, the B-wing symbol, DCX, Fabric OS, and SAN Health are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.