Digital Enterprises Require a Next-Generation Wireless Assurance Platform

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
By Shamus McGillicuddy
January 2018
# Table of Contents

Executive Summary ................................................................................................................................. 1  
Digital Enterprises Face Wireless LAN Assurance Challenges ............................................................. 1  
  The Wi-Fi Troubles That Keep You Up At Night .............................................................................. 1  
    Nightmare #1: Device Growth ........................................................................................................ 1  
    Nightmare #2: User Expectations ................................................................................................... 1  
    Nightmare #3: Budget Crunch ......................................................................................................... 1  
    Nightmare #4: Hackers and Inside Threats .................................................................................... 1  
The Ideal Approach to Wireless Assurance ....................................................................................... 2  
The Path to Wireless Assurance Success ............................................................................................ 2  
  Step #1: End-to-end visibility from a consolidated platform ............................................................ 2  
  Step #2: Granular and contextual data collection ............................................................................. 2  
  Step #3: Data retention—back-in-time visibility ............................................................................ 3  
  Step #4: Guided remediation ............................................................................................................ 3  
EMA Perspective .................................................................................................................................... 3  
About Cisco ........................................................................................................................................... 3
Executive Summary
The wireless LAN is increasingly the critical means of network access for enterprises today. With critical applications and business services relying on it daily, network managers have very little margin for error in wireless assurance. Unfortunately, many enterprises rely on fragmented and ineffective wireless assurance solutions. This white paper explores why wireless assurance is a business imperative and offers some advice on how network managers can find the right tools for success.

Digital Enterprises Face Wireless LAN Assurance Challenges
The modern digital enterprise will succeed or fail based on the quality and performance of its wireless LAN, particularly as digital leaders advance mobility and Internet of Things (IoT) initiatives. Network managers will need comprehensive wireless assurance solutions that can detect, analyze and troubleshoot Wi-Fi fault and performance problems.

Wi-Fi networks are essential for supporting enterprise mobility and bring-your-own-device (BYOD) initiatives. EMA research has found that 46% of network managers view mobility and BYOD support as an “important” or “critical” objective.¹

Wi-Fi networks are also important for delivering customer-facing applications and services. Retail companies rely on the Wi-Fi network to support points of sale and location-based services. Healthcare providers need Wi-Fi for support of patient care. Hospitality companies have guests who expect access to high-performing, highly available Wi-Fi. IoT also requires high-quality Wi-Fi connectivity. Sixty-three percent (63%) of network infrastructure professionals who support IoT say wireless LAN connectivity is essential to their IoT plans.²

The Wi-Fi Troubles That Keep You Up At Night

Nightmare #1: Device Growth
Today’s network managers face a broad set of wireless assurance challenges. First, more devices are connecting to the network and more applications are traversing it. IoT in particular is a challenge. A significant number (26%) of network teams who support IoT say their monitoring and management tools can’t handle the sheer number of new devices hitting the network. And this is a problem. Seventy-seven percent (77%) say IoT will create “significant” or “very significant” network traffic growth over the next couple years, and 30% say bandwidth capacity is one of their biggest IoT worries.³

Nightmare #2: User Expectations
Users often have high expectations. The quality of their home Wi-Fi is usually excellent. And when they leave home, their devices connect to LTE networks with almost no change in user experience. This sets the bar high and lowers their tolerance for fault performance issues. The moment when those users roam from LTE to the corporate wireless LAN (WLAN) network is a moment of truth. If their experience degrades when they connect, they will complain or find a workaround. These high expectations will also impact user adoption of new, critical applications. If a poor wireless experience degrades the performance of an application, users will reject it.

Nightmare #3: Budget Crunch
IT budgets aren’t growing fast enough to keep up with these demands, and many network teams struggle with Wi-Fi assurance as a direct result. Network teams need the resources to deliver comprehensive wireless coverage and acquire tools necessary to manage WLAN health and performance. Thirty-three percent (33%) of network managers reported that WLAN upgrades were a leading driver of their network monitoring and management decision-making. But 24% of all network managers said that a lack of budget and resources is their top challenge to network operations success.⁴

¹ Unpublished EMA survey research, 2015.
Nightmare #4: Hackers and Inside Threats

Security threats are constantly increasing and evolving, and the WLAN is a target. WLAN security tools are the number one investment for network managers who support BYOD/user mobility (44% of all network managers surveyed). IoT makes these security risks even scarier. Nearly one-quarter of network managers who support IoT said rogue device detection is a top challenge of IoT monitoring, and 52% said that IoT had introduced or worsened blind spots in their network monitoring and service assurance architecture. Two of every five network managers struggling with IoT blind spots reported experiencing a security breach.

The Ideal Approach to Wireless Assurance

Network managers who consider effective wireless assurance critical to digital survival should demand a solution that enables them to do the following:

- Isolate a problem quickly—ideally before end users are affected
- Replicate that problem in data if it is intermittent
- Resolve the problem decisively so that it doesn’t reoccur

The Path to Wireless Assurance Success

EMA recommends that network managers find wireless assurance solutions that can address these three critical needs. Network managers should look for assurance solutions that provide end-to-end network visibility on a consolidated platform, granular data collection across the network, deep data retention for replication of intermittent wireless issues, and analytics for guided remediation.

Step #1: End-to-end visibility from a consolidated platform

Network managers need end-to-end context when monitoring and troubleshooting the wireless network. This means that they need a client view to understand how endpoints are impacting quality of experience. Information about the user allows them to quickly understand if the user is connecting to the wrong network or accessing applications they have no rights to access. They also need to know what’s happening on the WAN and the Ethernet LAN backbone to isolate any problems to the right network. Finally, they require insights at the application level to understand which applications are performing well on the network.

But today’s network operators often use fragmented toolsets for wireless assurance, and this puts them on the wrong footing. Thirty-four percent (34%) of network managers use 11 or more tools for network monitoring and troubleshooting. This tool fragmentation leads to ineffective network operations because network managers spend too much time on data correlation, toggling between screens. EMA research has shown the consequences of this. On average, network operations teams detect 60% of problems before end users experience them and report them to IT. However, network teams that use 11 or more tools detect an average of only 48% of problems. They are more often in a reactive troubleshooting posture, and end users suffer while engineers go through lengthy diagnostic exercises.

Step #2: Granular and contextual data collection

Wireless assurance solutions should collect a broad and granular set of data. Granular data collection ensures that all events are captured, no matter how brief. Tools that rely on intermittent data collection (e.g., SNMP polling) will miss events that have an impact on user experience.

Broad, contextual data collection gives network managers the end-to-end insight they need to discover correlations and isolate problems. This data collection should include network telemetry from wireless access points, switches, and routers; identity and access policy data on users; Radio frequency (RF) data from wireless sensors; application insights from deep packet inspection tools technologies; and policy lists.

Granular and contextual data collection enables proactive troubleshooting, especially when components of the network infrastructure can act as sensors. Network devices can simulate end-client transactions like web browsing, and then the assurance solution can analyze this simulated traffic to predict network fault and performance issues before actual end users are affected.

---

5 Unpublished EMA survey research, 2015.
Step #3: Data retention—back-in-time visibility
Many wireless assurance problems are caused by intermittent or one-time errors or failures. RF interference generated by a microwave oven is a classic example. Engineers spend the majority of their troubleshooting efforts on replicating problems caused by such intermittent issues.

Wireless assurance solutions with data retention allow network managers to go back in time and look at the problem when it occurred. The more data retained, the less likely engineers will need to replicate past problems.

Step #4: Guided remediation
Network managers must leverage the power of advanced analytics to improve operations. New analytics solutions can help IT trace the root of a problem and determine the right actions to remediate it. With support for proactive problem prevention, network optimization, and more, analytics can also enable network managers to move beyond reactive troubleshooting.

EMA research has found that 49% of network managers were actively applying advanced analytics to their network data to optimize infrastructure, improve security posture, and proactively detect problems before they impact the business. The top use cases for these analytics efforts were network security monitoring (38%), network optimization (30%), business process optimization (27%), and predictive network analysis (25%).

EMA Perspective
Based on years of research and industry analysis, EMA’s perspective on optimizing WLAN assurance tools and practices can help today’s digital enterprises meet customer expectations and organize more efficient and effective network teams.

Today’s network managers face overwhelming challenges to wireless assurance. Users have high expectations, device growth is exploding, and most IT organizations lack the budget to address this situation effectively. With multiple initiatives and business processes relying on the wireless network for success, network managers need to get wireless assurance right. Wireless assurance requires an end-to-end platform for visibility that leverages broad and granular network data collection, deep data retention, and advanced analytics for machine-assisted operations.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow’s digital opportunity today. Discover more at www.cisco.com/go/dna and follow us on Twitter at @CiscoEnterprise.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMAs clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3655.010218