



WHITE PAPER

Assuring Service Delivery Across Converged Wired and Wireless Networks

Sniffer Expert, an application module that is part of Sniffer Global, provides various alarms and diagnostics that help users to quickly find performance, security, and network-related issues in their wireless infrastructure. Sniffer Expert can help network managers zero in on issues that may be creating performance issues or presenting vulnerabilities within the wireless infrastructure.

Sniffer Expert can help to alert on the following conditions:

- Rogue Access Point, Rogue Mobile Unit
- Association Failure, Authentication Failure
- Missing Fragment Number
- Same Transmitter and Receiver Address
- No Encryption, Open Authentication, or WEP Authentication Set for Access Point
- Weak Signal Strength for Access Point
- Too many clients connected to Access Point
- Access Point is broadcasting ESSID
- Stations connected in Ad Hoc Network

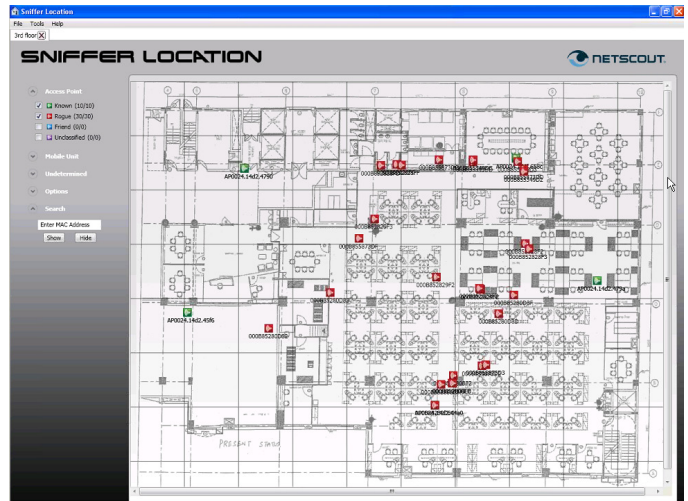


Figure 4. Location maps show where problems with mobile devices are occurring.

This location information coupled with traffic statistics and analysis dramatically increase the network manager’s ability to quickly resolve issues within the wireless infrastructure.

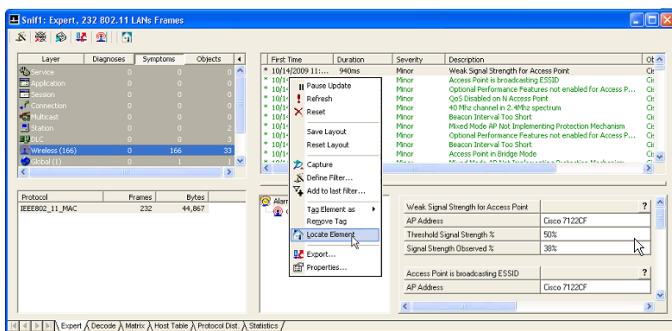


Figure 3. Sniffer Expert helps diagnose common wireless problems such as weak signal strength.

Figure 3 shows Sniffer Expert for Wireless. From this view, users can select an option to “show the location” for that device!

By viewing the wireless activity on a physical map, the network team can quickly see what devices are communicating, who they are communicating with, where the wireless traffic patterns are congregating (and misbehaving), and what other devices may be contributing to the problem.

A map can highlight where a single device is located or identify the physical location of different types of wireless devices (Figure 4).

Location viewers can also indicate a specific wireless communication in progress or quickly and easily see where communicating stations are clustered.

The location viewer allows users to quickly and easily see where communicating stations are clustered.

The network manager can then correlate this location information to statistical information such as traffic volume (bytes/packets in/out), retries, signal strength and quality, packet loss, association / disassociation, or authentication.

Sniffer Global – the Portable Analyzer with Enterprise-Class Security

Sniffer Global provides network managers with centralized management, allowing for tight user access controls and comprehensive activity logs. Since Sniffer Global is centrally administered, security is greatly enhanced ensuring a secure solution that offers powerful analysis tools without compromising network and application security policies. Most traditional portable network analyzers lack centralized security, and have virtually no control over what network data the user of the portable analyzer has access to. Sniffer Global allows your team to troubleshoot application problems without potentially exposing your data without checks and balances such as authentication and audit trails. When leveraging Cisco MSE location services, Sniffer Global speeds your time-to-knowledge by pinpointing the exact location of wireless problems. This aids network managers in quickly locating, identifying and resolving service-affecting problems – increasing service reliability and improving return on investment.

Monitoring the Wire in Wireless

While the enterprise-class Sniffer Global solution is designed to provide expert insight into 802.11 a/b/g/n lower layer issues such as signal strength and quality, packet loss, association / disassociation, authentication and others (Figure 5), there are many “wired-side” related protocols that also require visibility. Both wired and wireless clients access the same business applications on the wired back-end infrastructure. This is where the entire nGenius Service Assurance Solution comes into play. And while Sniffer Global with Cisco MSE integration provides network managers with the wireless insight they need to quickly resolve performance issues on the wireless side of the network, NetScout’s Service Assurance Solution provides a seamless performance management solution for assuring application delivery and network performance for the entire enterprise.

Host	Host Addr	Monitored Topology	Monitored Channel	Valid Topology	Valid Channel	Signal Cur	Signal Max	Signal Min	In Bytes	Out Bytes	In Pkts	Out Pkts
01087000000	G:OFDM	0		0		0	0	0	4,838	0	0	0
01087000000	G:OFDM	11	102.20	11	102.20	0	0	0	2,574	0	0	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	2,030	0	190	10
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,930	0	180	12
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	4,929	0	48,815	6
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	2,009	0	190	10
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	2,900	0	2,900	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	2,900	0	2,900	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,619	0	53,874	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	2,986	0	15	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,710,110	0	4,314	6,756
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	13,627	0	9,374	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	254	0	98,164	16
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	692	0	48,879	26
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	18	0	34,900	5
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	140	0	52,858	10
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	3	0	30,132	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	0	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	232	0	62,596	6
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	18	0	254	5
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	130	0	44,543	2
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	21	0	48,879	26
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	43,210	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	3	0	863	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	232	0	0	1
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	501	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	297	0	0	1
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	643	0	0	6
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,214	0	0	6
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,125	0	0	6
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	146	0	0	1
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	829	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	66	66	595	240
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	254	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	9,244	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	1,457	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	624	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	45,660	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	112	0	84,390	8
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	28	0	7,572	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	790	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	0	4
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	9,225	0
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	3,723	3,723	1,096	19
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	1,959	0	1,959	39
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	13,822	2
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	5,264	5,264	1,865	27
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	14	0	232	1
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	0	0	0	3
01087000000	G:OFDM	11	102.20	11	102.20	21	65	0	8,201	0	0	37

Figure 5. Sniffer Global provides expert insight into 802.11 a/b/g/n lower layer issues such as signal strength and quality, packet loss, etc.

Over the past few years major advances in usability and security of WiFi protocols have brought wireless into the enterprise mainstream. Much of the wireless network traffic runs on the back-end wired infrastructure for enhanced roaming, management and location services (i.e. Cisco MSE). Supporting all common wireless traffic protocols, the nGenius Solution provides unmatched visibility for wireless service delivery assurance, performance monitoring and optimization, and problem isolation.

The nGenius Service Assurance Solution is an end-to-end solution that enables always-on network and application performance management. Targeting the foundation technology infrastructure, the nGenius Solution provides comprehensive, service-level views into the overall health and performance of the backend infrastructure and applications supporting wireless service delivery. Using the nGenius® Service Delivery Manager intelligent early warning capabilities, IT staff can be alerted to emerging performance problems allowing the prevention and rapid resolution of service delivery degradations or interruptions. Highlighted capabilities include:

- Extensive network and application performance management
- Highly granular problem isolation capabilities
- Predictive alarms and event notification
- Voice-over-IP (VoIP) convergence management
- Policy validation and capacity planning
- Support for common wireless traffic protocols

Putting it All Together – The KPI-to-Flow-to-Packet Approach

NetScout's products leverage deep packet inspection technology to deliver complete visibility into real-time operational intelligence spanning high-level KPIs (Key Performance Indicators) and early warning notifications all the way down to actual packets, enabling IT organizations to accelerate problem resolution. The nGenius Performance Management System provides an easy pathway to progressively and contextually drill down from key performance indicators such as response time or errors, to application flow data such as utilization, conversations or top talkers, and then to packet-level details – when necessary.

This KPI-to-Flow-to-Packet approach allows the network engineer to decide how deeply he needs to drill down to effectively manage and troubleshoot network and application performance issues. The NetScout Solution introduces the first complete and consistent visibility in high definition for KPIs to help in early detection of emerging network or application problems. KPIs in the enterprise networking environment help answer the most challenging questions, including:

- “How fast is each application running?”
- “Is that response time acceptable?”
- “Are there any errors for that application or network area?”
- “What is the success rate?”
- “Is voice quality acceptable?”

NetScout's KPI-to-flow-to-packet approach to troubleshooting answers these questions so problems can be averted or quickly corrected in enterprise networks.

Visibility into Wireless Traffic across the Wired Infrastructure

The nGenius Service Assurance Solution accelerates problem resolution and increases operational efficiency, enabling IT organizations to optimize the delivery of services over wired and wireless networks. Below is a discussion of the wireless protocols supported by the nGenius Solution, enabling service assurance for converged wireless and wired networks.

Light Weight Access Point Protocol

The Light Weight Access Point Protocol (LWAPP) is part of the Control and Provisioning of Wireless Access Points (aka CAPWAP) and was developed to standardize communications between Wireless Termination Points (Access Points) and Access Controllers (Wireless LAN Controllers). LWAPP was designed to remove the requirement for intelligent Access Points so they can become just a remote RF extension to a controlling WLAN switch or router. Client traffic flows from the Access Point directly to/from the Access Controller. All LWAPP communications can be classified into one of two types:

- LWAPP Control Channel
- LWAPP Encapsulated Data

nGenius Performance Manager monitors the LWAPP protocol by creating a custom application for both UDP 5247 and UDP 5246 for LWAPP_data and LWAPP_control traffic. Figure 6 shown in the Protocol Directory screenshot below.

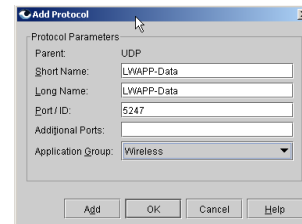


Figure 6. Adding new protocols is simple.

Inter-Access Point Protocol (IAPP – 802.1f)

The IETF 802.1f protocol is a standard for Access Point vendors to allow roaming compatibility between them. It uses the Inter-Access Point Roaming Protocol, which lets a roaming user transparently switch from one access point to another while moving around, no matter what brands of access points are used on the network infrastructure. In addition, this protocol dramatically improves roaming performance in order to allow multimedia or delay-sensitive applications to operate seamlessly.

The original IAPP used L2 messages between access points but did not support inter-subnet roaming. An enhanced “fast handoff” 802.1f IAPP provides a unified solution for both intra and inter-subnet handoffs. This enhancement is provided by utilizing an IP based IAPP or IP-IAPP.

The nGenius Solution can monitor 802.1f IAPP by creating a custom application definition for TCP and UDP port 2313 in nGenius Performance Manager.

Cisco Network Mobility Services Protocol

Cisco Network Mobility Services Protocol (NMSP) is the common protocol used between the Mobility Services Engine (MSE) and Wireless LAN Controllers (WLC). Cisco MSE provides the ability to track the physical location of any Wi-Fi device, including Wi-Fi clients, Wi-Fi active RFID tags, and rogue access points (APs) using Received Signal Strength Indication (RSSI) and Time Difference of Arrival (TDOA) technologies. Cisco NMSP replaces the legacy Cisco Location Protocol (LOCP). To monitor Cisco NMSP with the nGenius Solution, create a Server-Based Application in nGenius Performance Manager for the MSE appliance using TCP port 16113.

RADIUS

Many enterprise WiFi environments utilize RADIUS for authentication, authorization and configuration of wireless clients. Because it is important to have visibility into RADIUS communications, the nGenius Solution has built-in features that track RADIUS performance and error messages in real time using Key Performance Indicators (KPI).

The RADIUS protocol is enabled by default in Performance Manager and only requires minor configuration changes to start performance tracking. The screenshot in Figure 7 shows a RADIUS server in the new nGenius Service Delivery Manager service dashboard.

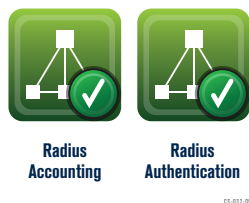


Figure 7. The nGenius Service Delivery Manager icons show that all is well with Radius Authentication and Accounting.

Monitoring a Cisco MSE Wireless Environment

In order to provide packet-level visibility and troubleshooting capability in a Cisco wireless environment, key components and aggregation points should be instrumented with nGenius InfiniStream appliances. Where possible, each Wireless LAN Controller (WLC) should be instrumented to monitor and capture LWAPP, NMSP and related traffic which will provide visibility into user, control and management traffic flows. The diagram in Figure 8 shows best practice visibility points in a typical backend wired infrastructure for ongoing performance monitoring and continuous packet capture of key devices in a Cisco Location-Based Wireless Infrastructure.

Conclusion

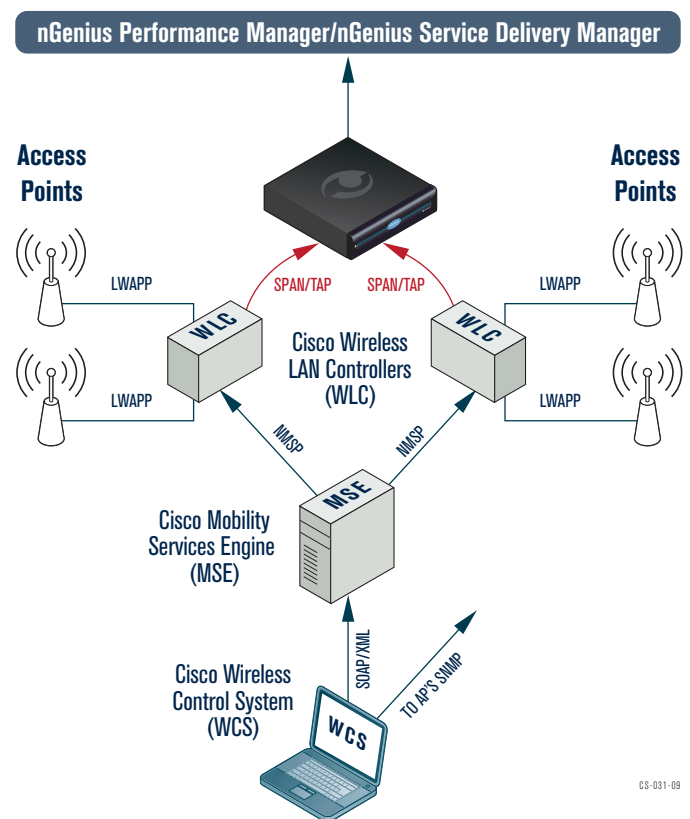


Figure 8. Best practice visibility points in enterprise wireless environments.

As wireless networks have evolved to become more critical to businesses than ever, IT organizations struggle to ensure service delivery over a wireless infrastructure. While similar service delivery management challenges exist in the wired domain, the wireless domain is always in motion, increasing the challenge of locating and isolating performance issues and security breaches. Using Cisco's innovative location services from the Cisco 3300 Series Mobility Services Engine, NetScout has integrated location-based information into its Unified Service Management portfolio to enable IT staff to rapidly correlate physical location with service and performance delivery.

Whether the requirement is for an always-on approach to managing the performance of technology infrastructure and the applications that supports the wireless environment, or if it is managing the wireless domain itself, NetScout solutions enable IT organizations to optimize, protect, and simplify the delivery of services over both wired and wireless networks. NetScout solutions help to identify security risks, predict and prevent performance problems and dramatically accelerate problem resolution. The result is a higher level of satisfaction and an improved quality of experience for network users, as well as increased productivity, greater operational efficiency, and improved cross-functional collaboration within the IT organization.



Corporate Headquarters

310 Littleton Road
 Westford, MA 01886-4105
 Phone: 978-614-4000
 Toll Free: 888-999-5946
www.netscout.com

European Headquarters

One Canada Square 29th floor
 Canary Wharf
 London E14 5DY
 United Kingdom
 Phone: +44 207 712 1672

Asia/Pacific Headquarters

Room 105, 17F/B, No. 167
 TunHwa N. Road
 Taipei, Taiwan
 Phone: +886 2 2717 1999



**For more information
 please visit www.netscout.com
 or contact NetScout sales at
 800-309-4804 or +1 978-614-4000**

©2010 NetScout Systems, Inc. All rights reserved. NetScout, nGenius, Sniffer, and InfiStream are registered trademarks and the NetScout logo is trademark of NetScout Systems, Inc. and/or its affiliates in the United States and/or other countries. Other brands and product names, and registered and unregistered trademarks are the sole property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.