# Managing Service Quality at the Network Edge

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Keysight
April 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

## EXECUTIVE SUMMARY

As enterprises shift more of their operations to branches or remote locations, network teams must ensure performance monitoring is extended to the network edge. With cloud computing, the Internet of Things, and other digital initiatives, data is frequently collected and used directly at the edge, never flowing through the network core. Too frequently, traffic at the edge goes unmonitored until a problem is reported. At that point the operations team must deal with the complexity and cost of isolating an issue about which they have little information. This white paper explores how comprehensive and cost-effective monitoring at the network edge is needed to reduce the risk of performance delays and outages at the edge of hybrid IT environments.

## NETOPS MUST MANAGE SERVICE QUALITY AT THE NETWORK EDGE

More than ever before, network operations teams need to be able to manage service quality at the network edge. Enterprises are becoming more distributed, with users in far-flung locations. Over the years, Enterprise Management Associates (EMA) research has observed a steady uptick in the number of remote sites connecting to wide-area networks and the number of devices connecting to the network within those sites. In fact, Internet of Things initiatives are driving up the number of network endpoints in remote sites and at the network edge, competing for bandwidth with end-user applications. Ideally, the network operations team needs to know the quality of experience at each of these edge sites.

Meanwhile, increased use of the Internet and cloud infrastructure has made monitoring more challenging. The average enterprise reports that 45 percent of network traffic is attributable to external cloud applications.[1] Additionally, more than half of enterprises (55 percent) connect their remote sites directly to public cloud services.[2] The network operations team has limited insight into cloud applications and cloud network performance because they have little to no administrative access to public cloud infrastructure, and thus a limited ability to extract meaningful performance data from the cloud. Thus, visibility into cloud performance is often lacking.

This visibility challenge couldn't come at a worse time. In today's digital economy, IT organizations have a mandate to deliver a high quality of experience. End-user experience has emerged as a top-four evaluation criteria for network operations success, as selected by 28 percent of network managers.[3] End-user experience correlation is the number-one most important feature of network performance monitoring tools today, selected by 33 percent of all network managers.[4]

Hybrid IT environments also exacerbate complexity. The network operations team is often the first line of defense for the end-user experience, even if the network isn't always the root cause of an issue. In fact, EMA asked network managers to identify the root cause of their most recent complex IT service problems that required cross-domain response across multiple groups in IT. The network was the top response (40 percent), but end-client system problems and user errors were also very common (total of 34 percent). Twenty-two percent of network managers identified public cloud service providers as the major culprit.[5] Enterprises need tools that can provide visibility into traffic at the edge to better manage services.

## THE JOURNEY TOWARD EDGE VISIBILITY

At a time when network edge visibility is becoming critical, many network operations teams lack the tools to acquire that visibility. The simplest and most affordable approach to gathering data at the network edge is to collect device metrics via polling protocols like Simple Network Management Protocol (SNMP). Of course, this only works for SNMP-capable devices, which excludes most laptops, smartphones, tablets, and IoT devices. The biggest limitation is that these metrics do not provide much insight into service quality. They are more useful for determining whether a network device or a network connection is up or down.

1 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
2 EMA, "Next-Generation Wide-Area Networking," July 2016.
3 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
4 Ibid.
5 Ibid.

Another common technique is network flow analysis. Flow records offer a summary of network traffic and provide insight into network performance and device status. Some organizations are successfully adopting this technique for monitoring the network edge. However, flow data alone does not provide the deeper insight needed to understand more complex issues. It offers summary data, not granular session data.

The most granular and valuable data for understanding the user's quality of experience are network packets. Packets captured passively from production networks are the best source of truth about what's happening at the edge. Packet aggregation solutions like network packet brokers can time-stamp and filter packet data, and deliver right-sized flows to monitoring tools for deep insight into network performance and the end-user experience. A packet broker that can see application-layer details, like the location of end-users, type of edge device, and the applications being accessed, offers additional value. This data makes it easier for performance engineers to identify the root cause of an issue and implement a solution that will prevent the issue from recurring.

Active monitoring of synthetic traffic is another valuable tool for monitoring service quality. Synthetic traffic can emulate the user experience at a remote site to test application performance. Active monitoring tools can monitor performance at times when users aren't generating traffic to anticipate performance degradations before they turn into problem tickets.

Recent EMA research confirmed that network managers are very focused on active monitoring and packet-based monitoring today. When EMA asked 250 network managers to identify the type of data they currently use for sustained network availability and performance monitoring, the top three responses were synthetic traffic (40 percent), management system APIs (40 percent), and packet inspection (35 percent).[6]

### Overcome Complexity and Scalability Challenges at the Edge

If an enterprise is using both passive packet monitoring and active synthetic monitoring solutions, the network team will usually have to deploy separate technology stacks at the network edge. This adds complexity to the overall monitoring architecture and introduces fragmentation in monitoring and management workflows. The challenge is amplified when the organization gets to the point where it must scale both solutions.

EMA research confirms that monitoring the edge with two separate technologies can be difficult. When EMA asked network managers to identify their biggest network operations challenges, a lack of end-to-end network visibility was their top response (24 percent). Twenty-two percent complained of fragmented management tools. Network teams need solutions that can integrate and consolidate monitoring infrastructure.[7]

## IXIA VISION EDGE COMBINES PASSIVE AND ACTIVE MONITORING AT THE NETWORK EDGE

Ixia, a Keysight company, introduced a solution that helps enterprises gain insight into service quality at the network edge. The Ixia Vision Edge products combine passive packet capture and network flow analysis with active, synthetic traffic monitoring.

Vision Edge is designed for deployment at remote sites and branch offices. The solution's packet broker capabilities enable network teams to capture and process NetFlow and packet data from production traffic and deliver groomed and load-balanced data to performance management tools for analysis. Thus, this tool enables network managers to gain insight into service quality at the network edge using production traffic. Vision Edge supports Ixia's NetStack, PacketStack, and AppStack software features for processing, filtering, and distributing relevant packet data to performance and security monitoring tools.

Vision Edge also supports active monitoring using the functionality of the Ixia Hawkeye platform. This solution produces synthetic application traffic for Layer 3 through Layer 7 verification from a vast library of common applications. Vision Edge sends that synthetic traffic to data centers and cloud applications, while Hawkeye observes network paths, response times, error rates, and more.

6 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
7 Ibid.

By blending passive and active performance monitoring, Vision Edge offers a consolidated view of service quality from a single solution deployed on the network edge. It consolidates visibility infrastructure and reduces complexity. EMA research has revealed robust interest in deploying network packet brokers at the network edge. Thirty-five percent of enterprises have deployed network packet brokers in remote sites or branch offices, and 30 percent plan to deploy them this year.[8]

With consolidated monitoring infrastructure, network operations teams can improve their end-to-end network visibility and reduce tool fragmentation. EMA research found that using network packet brokers and network visibility platforms typically enhances IT productivity, improves IT collaboration, progresses the network team's responsiveness to change, and accelerates the resolution of IT service problems.[9]

## EMA PERSPECTIVE

Digital enterprises that deliver critical applications and services at the network edge need an edge-centered approach to monitoring quality of experience. EMA research shows that they also need to analyze multiple data sources, including packets, flow data, and synthetic traffic, to develop a better picture of the end-user experience.[10]

Unfortunately, the deployment of multiple network and application monitoring tools at each remote location drives up cost, increases complexity, and creates tool fragmentation. Many IT organizations will be tempted to limit their tool investments at the network edge to avoid these issues. However, enterprises that give into this temptation will inhibit their ability to manage performance at the edge of the network.

EMA recommends that enterprises look for ways to consolidate monitoring infrastructure to control cost and complexity. Ixia Vision Edge solutions combine packet-based and active synthetic monitoring functionality in a single appliance. This technology can potentially reduce the cost and complexity of monitoring while providing the data necessary to improve service quality at the network edge. Distributed enterprises that need to increase their visibility into the end-user experience at remote locations should evaluate the new Ixia Vision Edge solution from Keysight and determine how it can benefit their business.

## ABOUT KEYSIGHT

Keysight Technologies, Inc. (NYSE: KEYS) is a leading technology company that helps enterprises, service providers, and governments accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster at a lower cost, with offerings from design simulation, to prototype validation, to manufacturing tests, to optimization in networks and cloud environments. Customers span the worldwide communications ecosystem, as well as the aerospace and defense, automotive, energy, semiconductor, and general electronics end markets. Keysight generated revenues of $3.9B in fiscal year 2018. In April 2017, Keysight acquired Ixia, a leader in network test, visibility, and security.

More information is available at www.keysight.com.

8 EMA, "Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics," August 2018.
9 Ibid.
10 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.

## 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 EMA's 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 blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

---



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

3818.040119


IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING