Los Angeles' IT Organization Adopts StableNet® for Network Monitoring

Executive Summary

The network operation center (NOC) for the city of Los Angeles had been investigating various network management platforms to gain adequate visibility into a complex municipal network. When it implemented StableNet® for infrastructure monitoring, it was able to shift from a reactive approach to network management to a proactive one. Moreover, the ability of StableNet® to customize its monitoring platform has proven to be invaluable to the city, especially when the NOC was asked to begin monitoring the addition of an Internet of Things (IoT) deployment.

HIGHLIGHTS

Vendor name: Infosim®

Product name: StableNet®

Product function: Network availability and performance monitoring

Vendor contact: www.infosim.net

The NOC Finds the Right Tool: StableNet®

Los Angeles' network operations team recently installed StableNet® for network availability and performance monitoring after years of reactive troubleshooting with multiple tools that were unable to provide end-to-end visibility into a complex and distributed network.

"We needed a visibility solution to manage connectivity, bandwidth utilization and performance," said Mike Frassrand, a network operations specialist for the city. "The scope of the project was to focus on network infrastructure devices and connectivity and to provide visibility to our NOC so it could be proactive in recognizing and remediating issues."

Throughout the years, Enterprise Management Associates (EMA) research has consistently found that end users detect and report 40% of network problems before the average enterprise network operations team is aware of them.[1] By the time an end user has filed a ticket, business processes and user productivity are already negatively impacted.

Since installing StableNet®, Frassrand has observed that network operations staff have increasingly opened trouble tickets proactively, allowing his team to address issues before end users and services are impacted. "We are definitely moving in that direction, detecting more problems before trouble affects users."

The city's NOC is responsible for managing more than 2,500 switches and routers spread over 700 sites and 450 square miles. The IT organization acquired StableNet® after it retired an outdated version of another network management solution.

Frassrand's team chose StableNet® for its ability to support fault management via SNMP polling and IPSLA testing. The platform's root-cause analysis engine, which uses its understanding of infrastructure dependencies to filter out alarm storms and identify problems quickly, was particularly valuable to the organization. The NOC's previous tools did little more than give the team up-down notifications on network devices. StableNet® gave them a workflow for fault management, allowing them to detect problems quickly, before users were aware of them.

[1] EMA, "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Cloud, and Advanced Network Analytics," April 2016.

The StableNet® discovery engine gave the NOC visibility into network changes, alerting it to new devices and device configuration changes, an essential feature for a city where multiple agencies might install their own equipment without notifying the IT organization. Many city agencies run their own networks, and they make frequent changes independently.

This new level of visibility into the network should deliver added value to the city over time. For instance, Frassrand believes that StableNet® will support his team's ability to collaborate with the security operations team when responding to security incidents. "We will be able to use it to determine the scope of a security incident and to isolate it," he said. "When the security team calls, we look at our alarms immediately to see if anything is out of baseline. Having the visibility provided by StableNet® will be of value to the city."

The city's NOC team also liked StableNet® Embedded Agent (SNEA), which is deployable as software or on a Banana Pi appliance. Deployable at the edge of a network, SNEA agents can generate active test traffic, which StableNet® can utilize to analyze client-side visibility into network health and performance. The SNEA devices proved to be the key to establishing critical visibility into an IoT project implemented by a public safety agency.

An IoT Project Created a Network Visibility Problem

One of the city's public safety agencies deployed wearable devices to its employees. At the end of each day, those workers would plug their devices into docking stations distributed throughout the city so that the devices could upload large media files to the cloud. Unfortunately, this type of technology had very little inherent ability to validate whether the docking stations were successfully sending data to the cloud. It became the NOC's job to assure that these IoT devices had connectivity.

"The docking stations don't do much to reveal a problem," Frassrand said. "If the LED indicator is red, that's how they know if they're having a problem."

The docking stations were connected to the city's fiber optic network. Traffic from the stations would pass through a central router, then through a firewall, and finally out into the cloud through a 10 Gbps internet connection. Given that the devices were non-traditional endpoints, IT monitoring tools lacked any inherent visibility into whether they were successfully connecting to the network.

"We had no monitoring [of the docking stations], so we wouldn't know if there was a problem until the public safety agency was aware," Frassrand said. "We were completely in reactive mode. We had one failure in transport where the cause was a fiber failure. It took us a day to work it out – way too long."

Infosim® Helped City Customize StableNet® for IoT Monitoring

Infosim® is known for its ability to customize its solution for unique monitoring requirements. At the city's request, Infosim® wrote custom scripts for the SNEA agents that enabled them to simulate the traffic generated by the docking stations. The network team installed SNEAs at each site where the docking stations were installed.

The SNEAs emulate the traffic that the docking stations generate when they upload media files to the cloud. The agents can then report the performance of that synthetic traffic to StableNet®, which in turn can proactively alert the NOC of any connection failures or network performance problems, saving valuable time and resources.

StableNet® also helps the NOC monitor how the docking stations impact overall network capacity, giving them visibility into how much bandwidth the solution consumes, versus other applications such as Microsoft Office 365. This is critical because the NOC wants to closely manage overall bandwidth utilization as the traffic from the wearable devices converges on the network with other applications. If

this converged traffic degrades the performance of a critical application, the IT organization invariably looks to the NOC for answers.

Prior to using StableNet®, monitoring and troubleshooting the wearable devices and their docking stations' network connections was "very crude and very painful," he said. "Now we're at the point where we're getting actionable alerts [in StableNet®] that we can respond to."

EMA Perspective

Enterprise Management Associates (EMA) research has found that network managers spend more than two-thirds of their typical workday fixing IT service problems.[2] Much of that time is spent in reactive troubleshooting mode. As noted earlier, 40% of all network problems are detected and reported by end users before the NOC is aware of them. Network managers can do better, but they need the right monitoring tools.

And network managers need better monitoring tools now more than ever. By all accounts, IoT will result in billions of new devices connecting to networks throughout the world. EMA research has found that 87% of enterprise network management professionals are providing network connectivity to IoT devices today.[3] Like it or not, network managers will often bear responsibility for assuring the health and performance of IoT network connectivity.

Many network operators will find that their incumbent monitoring tools are not up to the task of IoT service assurance. In fact, EMA research found that the number one challenge that network managers face with IoT is limited monitoring of connected IoT devices (44% of network managers who support IoT). Furthermore, 40% of network managers said they have installed new performance monitoring systems in response to IoT.[4]

Infosim® is an excellent example of a network monitoring vendor that provides the visibility network managers need to be more proactive with their networks. And Infosim® also has the technology and expertise to overcome some of the IoT monitoring challenges that network managers face. With minor customization of its SNEA agent, StableNet® was able to deliver visibility into wearable devices and their docking stations, solving a critical IoT monitoring problem.

[2] EMA, "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Cloud, and Advanced Network Analytics," April 2016.
[3] Ibid.
[4] Ibid.