SOLUTION BRIEF

Application Intelligence Reduces Troubleshooting Time and Costs

Make Network Troubleshooting Faster

Network engineers often struggle with where to start the troubleshooting process and is there a way to be proactive about troubleshooting. Application intelligence uses context-aware data processing to help with both concerns.

One key component of problem resolution is problem identification. Zeus Kerravala, Principal Analyst at ZK Research asserts that, “Problem identification is IT’s biggest challenge.” He explains that 85% of the mean time to repair (MTTR) is the time taken to identify that there is in fact, an issue. Even worse, the MTTR clock starts ticking whether IT knows there is an issue or not.

A second component of problem resolution is identifying the location of the problem(s). It is one thing to try to find the needle in the haystack. But which haystack should you even be looking at (network equipment, network applications, virtual data center, cloud provider, user/customer premises equipment, etc.)?

A visibility architecture that uses application data can be used to capture critical information needed for the whole troubleshooting process.

According to Zeus Kerravala, principal analyst at ZK Research, 85% of mean time to repair (MTTR) is the time taken to identify that there is in fact, an issue.

Troubleshooting and Application Intelligence

When there is an outage or service is degraded, it is not always easy to determine the issue. Identifying a common denominator among the people having a problem is important to minimizing outage durations. The problem could be that you have a bug in the new software you just released and it adversely impacted all Windows 10 workstations with Internet Explorer, or another specific browser platform. Instead, maybe a regional vendor released new code that is causing problems for customers in particular geographies.

KEYSIGHT TECHNOLOGIES

The key is to investigate rich metadata which can provide a lot of context about the user's connections to help you quickly isolate issues. With the right network packet broker (NPB), you can filter data based upon: application signature (and granular application actions), application bandwidth consumed, geographic location information, browser types in use, and device types in use. Some examples of questions that can be answered by rich metadata include:

- Is there an application failure on the network?
- Is there a geographic or service provider connection for loss of service?
- Are there unusual, or increased, usage of specific application features (play, pause, repeat, skip, etc.)?
- Are there unusual increases or decreases in application traffic?
- Is there a browser (e.g. Chrome) or device (e.g. Apple iPhone) related issue?
- Do you have the proper packet captures (PCAPs) that you need for debugging?
- Is the problem related to encryption, or is encryption making the problem harder to understand?

Proactive Problem Resolution Example

The use of metadata not only makes traditional troubleshooting efforts better but it allows IT to become proactive. Consider a traditional example using context- aware data processing functionality. A user calls in to the technical assistance center to report that their online gaming service does not work today. The gaming company representative looks at their servers and equipment but everything is okay. The gaming company also has not received widespread complaints in the last 48 hours. The next step is to start troubleshooting with the individual. The technician resets the customer account data but nothing happens. Next, the technician will now spend lots of time trying to figure out what the problem is. This is happening for several customers but it is still not a widespread issue. By using available application data, the gaming company network operations center (NOC) could quickly have seen that there are multiple complaints from one geographic area. They could then have narrowed it down to one ISP (ABC cable company). Then the gaming company could have called that one ISP and found out that they performed a software update during the night. This update will end up being the source of the problem that needs to get troubleshot—not the individual customers.

The proactive version of this example would look like the following. A NOC engineer uses metadata to observe that there is an unusual drop in application traffic on their network for the gaming app. This is a possible indicator of an issue. The engineer then looks for any sudden geographic drops in traffic usage. The person sees that there is a geographic area where all gaming activity has ceased. The representative can then capture the autonomous system (AS) information allocated to each specific internet service provider (ISP) using the border gateway protocol (BGP). That information is then sent to a NetFlow collector. A packet capture (PCAP) file can also be created to capture the metadata information for further analysis correlation. This makes it really easy for the engineer. They pull up the PCAP file, decode it using Wireshark, and then use the information to observe the fault and begin resolution, often before customers even know there is a problem.

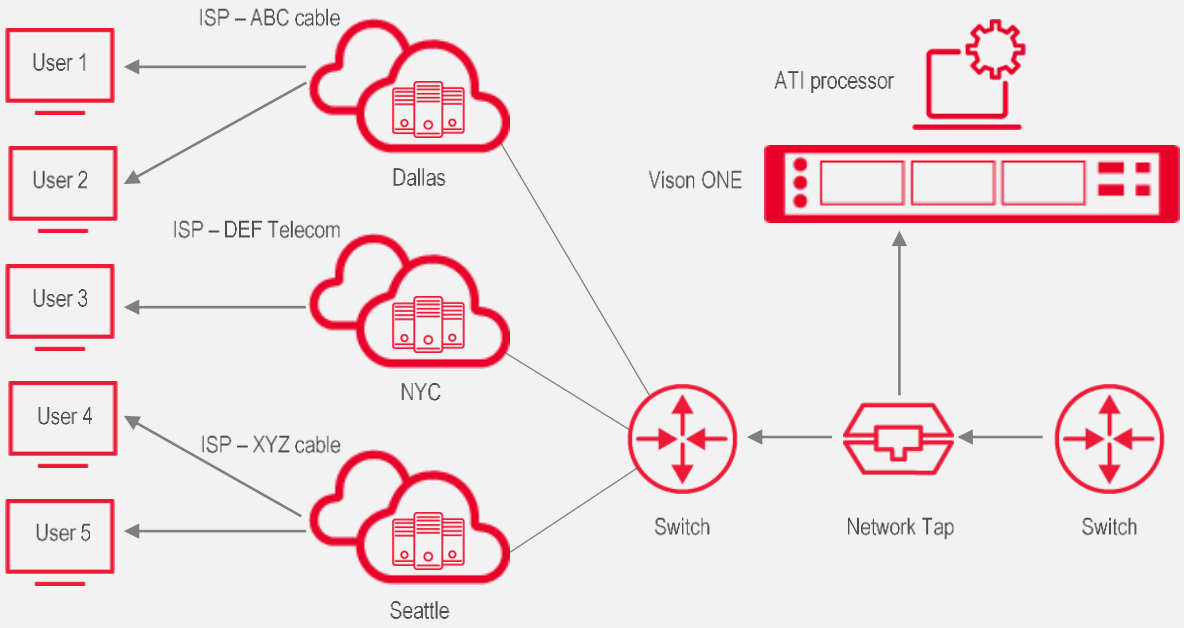

Figure 1. Example of a visibility architecture using application intelligence to detect geographic locations for outages.

Summary

Keysight can not only improve, but also simplify, your troubleshooting activities by using context-aware processing to analyze and report on your application data. The Keysight solution contains additional information including geolocation, browser type, device type, BGP Autonomous System numbers for ISPs, and other information. Instead of attempting to “find the needle in the haystack” within all of your web traffic, the metadata provided by Keysight helps you to rapidly and uniquely identify suspicious traffic or activity and drill down to see defining characteristics that reveal further insight on network impairments. Keysight was first to market with these metadata capabilities in 2014 and we have continued to enhance these capabilities to deliver actionable intelligence.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES