APPLICATION NOTE

Quick Tips to Improve Network Troubleshooting

According to the Enterprise Management Associates report, Network Management Megatrends 2016, IT teams spend nearly 36% of their daily efforts on troubleshooting. This is for good reason. Figuring out why your network and applications are not behaving as expected can be one of the most high-profile and aggravating activities there is for IT personnel. Pressure increases exponentially on IT personnel as problem resolution times increase, since this time factor directly correlates to network and application slowness and downtime.

One foundational solution is to create a visibility architecture. This allows you to improve troubleshooting activities by:

- Reducing the need and quantity of Change Board approvals
- Capturing more precise data for monitoring tools
- Implement better techniques like data filtration and floating filters

A visibility architecture is an end-to-end infrastructure which delivers network, application, and security visibility. This visibility is what allows you to optimize your network data capture and analysis techniques. A visibility architecture typically yields immediate benefits like the following: eliminates blind spots, improved data flow to security tools, and maximum network and tool availability.

There are three layers to a visibility architecture. The first layer is **data access**. This is where you will want to insert taps into the network between the network data flow and your monitoring tools (or network packet broker) to improve the quality of monitoring data and time to data acquisition. Once the tap is installed into the network, it is a permanent passive device that gives you data access. This means you don’t have to ask the Change Board for permission to touch the network again. You touch it once to install the tap and then you are done.

The second layer is the **monitoring data manipulation layer**. This is where you will want to deploy network packet brokers (NPBs) between those taps and the security and monitoring tools to optimize the data sent to the tools. Once installed, you can perform out-of-band data filtering, deduplication, packet slicing, header stripping, and many other functions to optimize the data before it is sent to your monitoring and security appliances. Just by implementing taps and NPBs, it is possible to reduce your mean time to repair (MTTR) by up to 80%. A significant portion of that time reduction comes from the reduction (and probable elimination) of Change Board approvals.

Overview

This brief provides suggestions on how you can improve your troubleshooting activities.

Additional Resources

- How To Improve Network Troubleshooting Podcast
- Best Practices for Network Monitoring

KEYSIGHT TECHNOLOGIES

The third layer of a visibility architecture consists of the **monitoring and security appliances**. Examples include protocol analyzers, packet capture (PCAP) solutions, and network analysis tools.

While the right tools can help you reduce your troubleshooting time, the visibility architecture itself has additional benefits. For instance, once you have your visibility architecture in place, there are several possible ways to optimize your troubleshooting workflows. Here are some examples:

- Deploy NPBs that support floating filters to further decrease the time to data acquisition. Floating filters are preconfigured filters. They can be configured to capture specific types of data and feed that data to specific tools, like Wireshark. Since the filter is preconfigured, the time it takes to activate the filter can be on the order of only one minute. This means a significant reduction in the time for data captures.
- Use NPBs that support adaptive monitoring. Automation using a RESTful interface to devices like a SIEM can minimize the time required for data captures.
- Implement proactive troubleshooting with application intelligence to create a macroscopic troubleshooting approach that reduces fault localization time. Application level information can be used to localize geographic and macroscopic network issues.

Just by implementing taps and NPBs, it is possible to reduce your mean time to repair (MTTR) by up to 80%. A significant portion of that time reduction comes from the reduction (and probable elimination) of Change Board approvals.

Visibility Architecture Solutions from Keysight

Network visibility solutions allow you to get a clearer picture (in a faster way) as to what is happening on your network. This allows you to reduce your MTTR performance.

Ixia's network visibility solution involves using NPBs in conjunction with application filtering and taps. Learn more about Keysight's taps, Network Packet Brokers, NetStack, and AppStack technology along with the solutions that our technical partners offer.

About Keysight

Keysight provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks for enterprises, governments, service providers, and network equipment manufacturers.

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