SOLUTION BRIEF

Floating Filters Dramatically Cut Data Collection Time

Deployment Scenario: Out-of-Band Visibility Architecture

When you are in a troubleshooting situation, minutes matter. According to the 2016 Cost of Data Center Outages study conducted by the Ponemon Institute, the average cost of a data center outage is $740,357 and lasts for about 95 minutes. This results in a cost of $7,790 per minute of downtime. So, when a network- or application-level event happens, a rapid response is needed to begin troubleshooting activities to limit outage costs.

Another data point from an Enterprise Management Associates report, Network Management Megatrends 2016, shows that information technology (IT) teams already spend around 36% of their daily efforts on reactive troubleshooting efforts. A key component to lightening this load and reducing the mean time to repair (MTTR) is to choose a network packet broker (NPB) that allows you to create floating filters for out-of-band monitoring data. Once a floating filter is created, it can be applied at will, which can save you several minutes (to more than an hour) of troubleshooting time.

Solution Components:

- Keysight Network Packet Brokers
- Keysight Taps
- Network Monitoring Tools

Benefits

- Reduce network downtime
- Reduce time spent on problem resolution
- Increase IT personnel efficiency

Solution Overview

This solution allows you to:

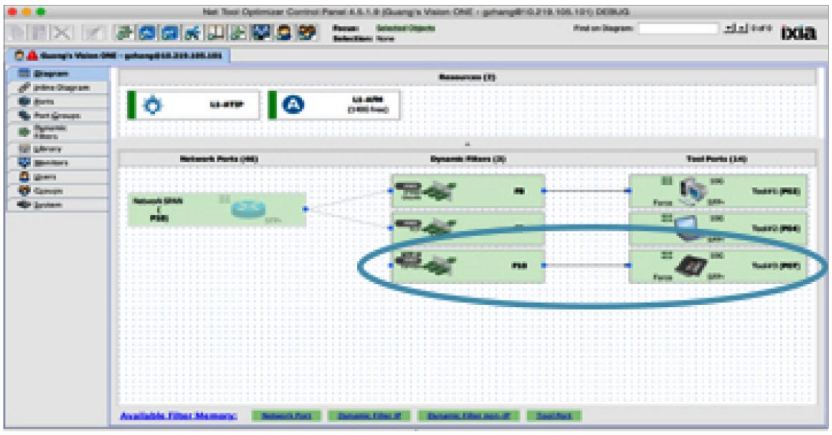
- Pre-stage monitoring data filters and connect them to standby troubleshooting tools (e.g., analyzers, Wireshark, Snort)
- Use a drag-and-drop interface in the NPB to connect a network port to a filter
- Start capturing data in less than 1 minute to reduce troubleshooting costs

KEYSIGHT TECHNOLOGIES

What are Floating Filters?

A well-designed visibility architecture allows you to organize your network monitoring strategy in such a way as to improve troubleshooting activities. At the core of this visibility architecture is an NPB. A good NPB will allow you to create unassigned monitoring data filters, also called “floating filters.”

These filters are called floating filters, because they are not attached to a network port, but they are attached to a monitoring tool—so they are free floating. The power of the floating filter is that it is already created and connected on the tool side. When needed, the tools can instantly be connected to a network port to analyze incoming data. This speeds up diagnosis time, since the forensic tools are already in standby mode.



A pre-defined filter can save you several minutes to more than an hour of time when compared to configuring filters manually using a command-line interface (CLI).

Reduce Time to Data by Using Floating Filters

As mentioned earlier, a rapid response is needed to control costs. A pre-defined filter can save you several minutes to more than an hour of time when compared to configuring filters manually using a command-line interface (CLI). A floating filter capability allows an administrator that is more experienced with the NPB product to create and pre-stage diagnostic filters, regulatory or industry compliance (such as Payment Card Industry (PCI) Data Security Standard (DSS) verification) filters, or other filter types. This ensures accuracy when compared to creating filters in a rushed environment where parameters can be missed.

An example use case involves using a Wireshark tool or a protocol analyzer. Any tool that is used often can be set up with a floating filter and pre-staged. A pre-defined filter can save you several minutes to more than an hour of time when compared to configuring filters manually using a command-line interface (CLI).

You simply draw a connection from the network to the port on the floating filter. It is that easy and takes less than one minute. If you need to make any filter adjustments, they are simple button clicks. In addition, the floating filters can be connected remotely by using a drag-and-drop interface on the NPB. This gives you 24 x 7 x 365 diagnosis capabilities from remote locations.

Any filters created for network or tool ports connected to the NPB can be saved to a filter library for quick reuse when desired. The filter library can also be pre-built by the IT organization for access whenever necessary—without requiring knowledge of detailed filter criteria, addressing, or specifics surrounding a scenario. This library is perfect for a junior engineer or third-shift staff. Filters can be saved with a single component field or a composition of several filter criteria fields that are combined using Boolean algebra with “and” or “or” actions, such as non–PCI compliant protocols on specific virtual local area network (VLAN)

Summary

Reducing network troubleshooting time is an important task for IT. Not only is uptime critical for the business, a faster reduction in troubleshooting times can demonstrate IT’s importance to the business and verifiable success for key performance indicators (KPIs).

Specific NPB filters for troubleshooting can be pre-staged and connected to standby troubleshooting tools. This can dramatically cut data collection times, as the troubleshooting filter simply needs to be connected to an incoming network port to the NPB. Once the connection is made, the tool can start capturing critical data in less than 1 minute to reduce troubleshooting time and costs.

Visibility Architecture Solution from Keysight

Keysight’s network visibility solution involves using NPBs in conjunction with application filtering and taps. Learn more about Keysight’s Network Packet Brokers and Tap technologies, along with our technical partner solutions.

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