SOLUTION BRIEF

Harnessing Network Visibility to Reduce Mean Time to Repair

Deployment Scenario: Out-Of-Band Visibility Architecture

While no one really likes network troubleshooting, it is an almost daily and time-consuming occurrence for information technology (IT) teams. According to the Enterprise Management Associates report, Network Management Megatrends 2016, IT teams already spend around 36% of their daily efforts on

reactive troubleshooting efforts. As a consequence, there has been effort directed over the years to reducing mean time to repair (MTTR).

MTTR is a direct measure of troubleshooting time. The lower this number, the better off a business, and its IT department, are. Higher numbers mean that it takes longer for the network to recover from a problem, and more of IT's time is spent fighting problems.

According to ZK Research, 85% of MTTR is spent just trying to figure out that there is, indeed, a problem. This is a lot of precious IT admin and engineering time.

There is a better way though. A network visibility architecture can be deployed that allows IT to install solutions that can access, aggregate, refine, and distribute critical troubleshooting data. This data can then be used to isolate and identify network problems as quickly as possible to restore optimal functionality.

Solution Components:

- Keysight Network Packet Brokers
- Keysight Taps

Benefits:

- Reduce network downtime
- Reduce time spent on problem resolution
- Meet or exceed problem resolution time KPIs

Solution Overview

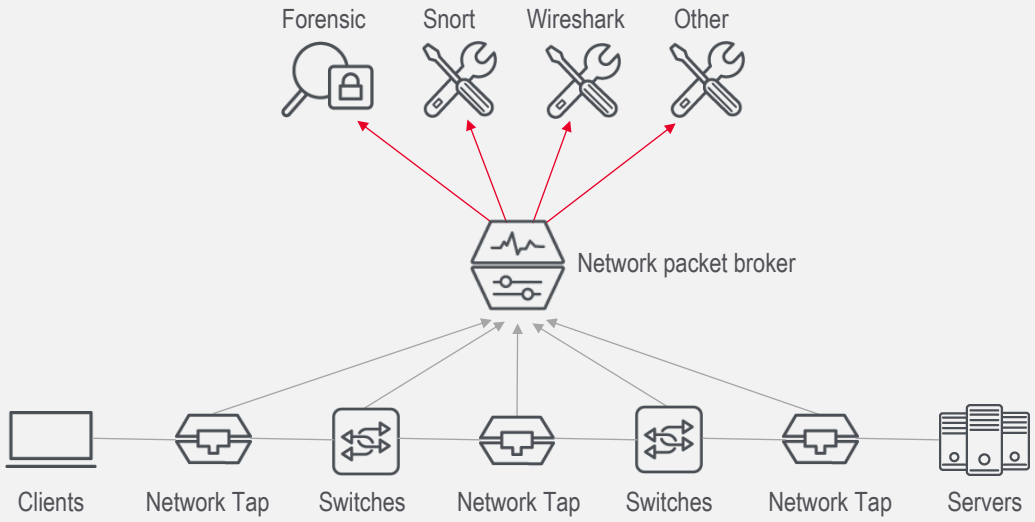
- This solution allows you to:
- Potentially reduce MTTR by up to 80%
- Expose hidden network blind spots
- Eliminate unnecessary technical roadblocks for troubleshooting
- Eliminate unnecessary process roadblocks for troubleshooting

KEYSIGHT TECHNOLOGIES

What Is a Visibility Architecture?

A visibility architecture is simply an out-of-band way to step back and take a look at your network, organize your network monitoring strategy, and then integrate that strategy with other strategies—like network security and troubleshooting. There are three basic components to a visibility architecture—the access layer, the control layer, and the traditional monitoring tool layer. In the past, people have typically said that the monitoring tools are the strategy. As a consequence, most enterprises have a mixture of many tools, several of which they do not even use; and that adds a lot of unnecessary complexity, and they still have a lot of network problems.

There are several specific use cases and instances where MTTR can be lowered by deploying the correct network visibility solutions.



The simplest solution is to deploy a network packet broker (NPB) with taps. Taps provide a complete copy of data, which can then be optimized (e.g., filtering, deduplication, Secure Sockets Layer (SSL) decryption) by the NPB and distributed to the requisite monitoring tools.

How Does a Visibility Architecture Improve Troubleshooting Efforts?

In regards to network monitoring, there are several specific use cases and instances where MTTR can be lowered by deploying the correct network visibility solutions. Here are some specific actions that can be taken:

- Reduce or eliminate the need for Change Board approvals
- Reduce or eliminate the need for crash carts
- Optimize monitoring data filtering
- Reduce time to data by using floating data filters
- Deploy NPBs that support adaptive monitoring
- Implement proactive troubleshooting with application intelligence
- Eliminate the use of network switch SPAN ports

There are several specific use cases and instances where MTTR can be lowered by deploying the correct network visibility solutions.

By eliminating Change Board approvals, the IT department can often start troubleshooting activities immediately. There is no need to wait minutes, hours, or days for approval to connect diagnostic equipment to the network, because it is already connected and ready to go.

Reduce Or Eliminate the Need for Change Board Approvals

Taps are passive devices and will not materially affect network traffic after they are inserted into the network. Security and monitoring tools can then be connected to the NPB at will. This can dramatically speed up troubleshooting diagnostic time, as many Change Board approvals can be eliminated. Change Boards typically govern the production network and oversee what activities can and cannot be implemented to the network. This is because these changes often cause network disruptions and outages. By eliminating these approvals, the IT department can often start troubleshooting activities immediately. There is no need to wait minutes, hours, or days for approval to connect diagnostic equipment to the network, because it is already connected and ready to go.

Reduce Or Eliminate the Need for Crash Carts

Once taps and NPBs are inserted into the network, no more network-affecting changes are needed, assuming the deployment was done correctly. Security and monitoring tools can then be connected to the NPB at will. This can dramatically speed up troubleshooting diagnostic times, as crash carts (special purpose carts with a collection of triage and troubleshooting tools) are no longer required. The tools are pre-connected to the NPB. This eliminates time spent locating the cart, moving the cart to the correct place, and inserting it into the network, reducing configuration time for the network tools. This can be especially pertinent if troubleshooting needs to be conducted on links and equipment in remote locations. MTTR reductions of up to 80% are possible simply due to the elimination of Change Board approvals and crash carts. By eliminating Change Board approvals, the IT department can often start troubleshooting activities immediately. There is no need to wait minutes, hours, or days for approval to connect diagnostic equipment to the network, because it is already connected and ready to go.

Optimize Data Filtering

Filtering of monitoring data is one of the most commonly used NPB features. It can significantly reduce the amount of unnecessary data sent to security and monitoring tools, which increases tool efficiency and allows them to scale. Filtering can be very granular to select only the data you need based on Internet Protocol (IP) address, virtual local area network (VLAN), etc. This speeds up time to resolution by the monitoring tool(s), as there is less "junk" to sort through.

Application intelligence uses application-related data to look at additional network data information. If this information is looked at in conjunction with trouble incident reports, then this can often shorten the time of troubleshooting.

Reduce Time to Data by Using Floating Data Filters

Specific NPB filters for troubleshooting can be pre-staged and connected to standby troubleshooting tools (e.g., analyzers, Wireshark, Snort). This can dramatically cut data collection times, as the troubleshooting filter simply needs to be connected to an incoming network port to the NPB. This can be done remotely using a drag-and-drop interface on 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.

Deploy NPBs That Support Adaptive Monitoring

Adaptive monitoring is the ability of the NPB to respond to network commands and make configuration changes. This automation capability improves monitoring response times by being able to respond to network incidents with actions in near real-time. Commands can be received using a representational state transfer (REST) interface from network management systems (NMS), orchestration systems, security information and event managements (SIEMs), etc. Faster responses to problems result in a shorter mean time to diagnosis and corresponding faster MTTR.

NPBs can also be integrated with SIEMs to automate threat detection and mitigation. This allows the NPB to respond to SIEM REST calls. A faster response time to problems results in faster incident detection, faster MTTR, and reduced network security risks.

Implement Proactive Troubleshooting with Application Intelligence

An NPB can be equipped with application intelligence. Application intelligence uses application-related data to look at additional network data information. For instance, user geolocation, device type, browser type, border gateway protocol assignment (BGP AS) information, and application traffic change information can be used to help pinpoint problems. If this information is looked at in conjunction with trouble incident reports, then this can often shorten troubleshooting time. For instance, is the problem affecting all devices or operating systems or just specific ones? Are the incidents being reported from a single geographic area? Is the incident related to a specific carrier or Internet service provider? These data points can be very useful in diagnosing problems.

Eliminate The Use of Network Switch Span Ports

A hidden blind spot can be the use of Switched Port Analyzer (SPAN) ports. SPAN ports can drop data without any notification of the data loss. This includes corrupted data (like malformed packets, frame errors, etc.), which can be useful for troubleshooting. In addition, in switch overload situations, i.e., when there is often a network switch problem, SPAN port data can be dropped without notification, as this port has a lower priority than traffic ports. So, the critical troubleshooting data you want might not be forwarded to diagnostic tools, and you will never know unless you see data gaps or attach a network analyzer to the network switch to validate SPAN port output. A tap eliminates this issue, because all data is forwarded on to the NPB. At this point, you choose what data is removed or not removed.

Summary

Network troubleshooting can be likened to finding a needle in a haystack. The trick is to make the haystack as small as possible as quickly as possible. One of the best approaches to improving troubleshooting is to eliminate processes that slow down the troubleshooting effort, filter out non-relevant information, and analyze the remaining data as fast as possible.

A visibility architecture consisting of taps and NPBs provides the core features set you need to accomplish this goal. Keysight has documented case studies where customers have been able to reduce their MTTR by up to 80% after implementing a solid visibility architecture.

Visibility Architecture Solutions 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 technology, 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