APPLICATION NOTE

Quick Tips to Improve Network Performance

According to research conducted by Enterprise Management Associates in October of 2016, 41% of IT personnel spend over 50% of their time working on network and application performance problems. This is further compounded by research that shows that tactical data loses 70% of its value after 30 minutes. This makes the speed and accuracy of monitoring data analysis critical. Network administrators need application monitoring tools to help them discover, isolate, and solve problems related to applications as quickly as possible.

Various parameters require analysis, including client CPU utilization, data throughput, bandwidth consumed, application memory consumed, and geographic location of problems. The fastest, most stable way to improve network and application monitoring is through better network visibility. A network visibility architecture enables you to see, isolate, and capture anomalies in your data flows. This leads to faster isolation of potential problems and improves end-user experience.

Once a visibility architecture is implemented, you will have access to additional forms of data. This allows you to improve performance monitoring activities by:

- Capturing performance-related data as fast as possible to get the best quality data possible
- Capturing the right types of data that you need and distribute that data to your purpose-built monitoring tools
- Harnessing the power of application intelligence to improve the quality and speed of your monitoring and analysis activities

Overview

This brief reviews techniques to improve network performance by changing the way data flows.

Additional Resources:

- How to improve network performance Podcast
- Best practices for network monitoring

KEYSIGHT TECHNOLOGIES

A visibility architecture starts with 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.

The second layer is the monitoring and data manipulation layer. This is where you will want to deploy network packet brokers (NPBs) between those taps and the network and application monitoring tools to optimize the data sent to those devices. Once installed, an NPB 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.

The third layer of a visibility architecture consists of the monitoring devices. A Network Performance Monitoring (NPM) solution is comprised of tools that can take metrics from your baseline analysis, flow data, and information that can come directly from your network devices to give you a complete picture

of your network. Examples include protocol analyzers, NPM, application performance monitoring (APM), network monitoring system (NMS) solutions, and network analysis tools. However, standalone deployments (without using an NPB) of these tools can run into problems like: overloaded disk space and processing, the need for different interface ports based upon network traffic speed, and the need for unnecessary data capture ports across the network.

Once you have your visibility architecture in place, there are several possible ways to optimize your network and application performance monitoring activities. Here are some examples:

- Deploy NPM solutions inline using external bypass switches to capture real-time data flows
- Use application intelligence within the NPB to identify slow or underperforming applications
- Leverage application intelligence to prevent application bandwidth overloads on your network
- Implement proactive monitoring to create better and faster network rollouts

By deploying NPM solutions inline, an external bypass switch can capture real-time data flows, allowing you to resolve data delivery delays for redundant and simultaneous data paths.

Hardwiring network connections can run into problems like:

unknown overloading of disk space and processing, inability to change interface ports based on network traffic speed, and the need to have more input ports to capture data across the network.

When application intelligence is incorporated into the NPB, it lets you capture application data across your network. Once you have this application data, you can identify slow or underperforming applications. For instance, application information, flow data, and geographic information can be combined to show what applications are running on your network, how much bandwidth each application is using, and what the geographic usage is per application. This solution allows you to isolate and filter traffic matching specific applications, geographies, keywords, and handset types. This data can then be exported to other applications, like a Splunk solution, for long-term data collection and performance trending.

Application intelligence information can also be used to predict user and application performance. A fundamental benefit of this solution is that you can see if there are any bandwidth bursts or explosions on the network. For instance, one mobile carrier a few years back had a situation where a new smartphone application was introduced. It was an interactive application between multiple users. Customers loved the app and usage skyrocketed. Over the course of a few weeks, the bandwidth consumed became exorbitant and the mobile carrier network actually crashed and was out of service for several hours. Application intelligence would have provided an early indication about the size of the application bandwidth and the rate of growth. IT personnel could have then used this information to limit the application bandwidth or usage.

Proactive monitoring is another way to improve performance. This solution uses visibility technology to actively test your solution either before rollout, during rollout, or after rollout. For instance, it can be used to provide better and faster network and application rollouts by pre-testing the network with synthetic traffic to understand how the solution will perform against either specific application traffic or a combination of traffic types. The synthetic traffic provides network and/or application loading simulations for a “busy hour” and the flexibility to perform evaluations during the network maintenance window. Ops and DevOps teams can validate their solutions with less risk using proactive monitoring functionality.

Visibility Architecture Solutions from Keysight

Network visibility is what enables you to quickly isolate and resolve performance issues; ultimately ensuring the best possible end-user experience. From there, you can use anomaly driven data flows to quickly isolate potential problems.

Keysight’s network visibility solution involves using network packet brokers in conjunction with application filtering and taps. Learn more about Keysight’s **Taps, Network Packet Brokers, AppStack,** and **Hawkeye** technology along with the solutions that our technical partners offer.

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