WHITE PAPER

Troubleshooting Network Quality of Service and Performance

How Network Visibility Can Help

You can't manage what you can't measure, and the same thing is true for quality of service (QoS) and performance issues on a network. All too often organizations are blind when it comes to network troubleshooting. Fortunately, it doesn't have to be that way. With an effective network visibility architecture, you can measure performance and identify the source of problems – reducing the time to resolution and driving a better user experience.

This paper outlines key network visibility topics that can help optimize performance, including, the following:

- application intelligence that identifies slow or underperforming applications
- application performance monitoring for network optimization
- proactive monitoring that creates better and faster network rollouts
- optimization of network performance monitoring effectiveness
- prevention of application bandwidth overloads on your network
- use of a GTP Session Controller to improve carrier customer quality of experience (QoE)
- improved and simplified voice quality monitoring efforts
- focused deep packet inspection that optimizes your network data
- inline network performance monitoring
- improved data collection that makes QoE monitoring more effective
- the offload of NetFlow data generation for improved switch performance

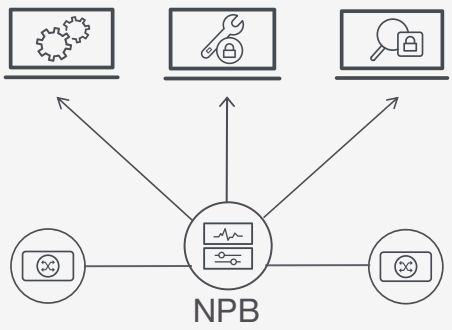
KEYSIGHT TECHNOLOGIES

Application Intelligence Identifies Slow or Underperforming Applications

Summary

- Use a network packet broker (NPB) with an application-level dashboard to observe applications in use and bandwidth consumption.
- Identify bandwidth hogs and bandwidth explosions such as smartphone apps.
- Use geolocation to show overloaded and underperforming network segments

Deployment scenario: Out-of-band visibility architecture



Solution overview

Application intelligence can identify slow or underperforming applications. For instance, application information, flow data, and geographic information deliver data that shows what applications are running on your network, how much bandwidth each application is using, and what the geographic usage is for the application. This solution allows you to isolate and remove traffic that matches specific applications, geographies, keywords, and handset types. You can export this data to other applications, such as a Splunk application, for long-term data collection and performance trending.

An NPB with application intelligence functionality allows you to access empirical data to identify bandwidth usage, trending, and growth needs. This empirical data enables you to proactively manage network resources and new equipment installations, accurately forecast expansions and improve budgeting for expansions.

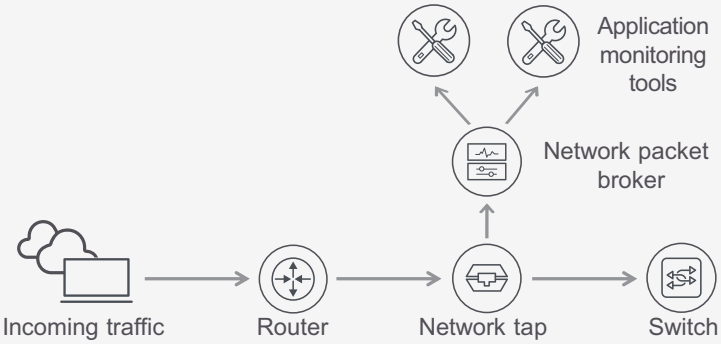
It is possible to export collected data as packet data or NetFlow information, depending upon the input required by your monitoring tools. The data can also be viewed natively in a dashboard for early access to the information and real-time analysis.

Application Performance Monitoring Delivers Network Optimization

Summary

- Many IT personnel spend a considerable part of their day working on network and application performance problems.
- Use an NPB with application performance management (APM) tools to quickly isolate and resolve application issues with better data monitoring.
- Validate service-level agreement (SLA) performance for network applications.

Deployment scenario: Out-of-band visibility architecture



Solution overview

One of the main tasks of IT is to ensure application availability across the network. This is a complicated task because of various parameters, including physical network effects, distributed employee network access, use of virtualization and cloud networks, assorted security threat controls, a multitude of device types, and network bandwidth limitations. Network administrators need application monitoring tools to help them discover, isolate, and solve problems related to applications. Various parameters require analysis, including client CPU use, data throughput, bandwidth and application memory consumption, and geographic location of problems. Some tools even allow you to drill down into the application code to get additional insight.

APM solutions allow you to understand the performance of critical transactions on your network and correlate the transactions and data across your network. This information can solve performance and availability issues. For example, a common blind spot for hospitals is access to application data and application performance trending. In this case study, the customer used the EpicCare Ambulatory Electronic Medical Record (EMR) application from Epic but had trouble correlating all the information from different systems. The customer deployed an NPB that was able to aggregate data from the relevant sources, filter out the correct out-of-band monitoring data, and then feed it to the customer's APM tool for analysis.

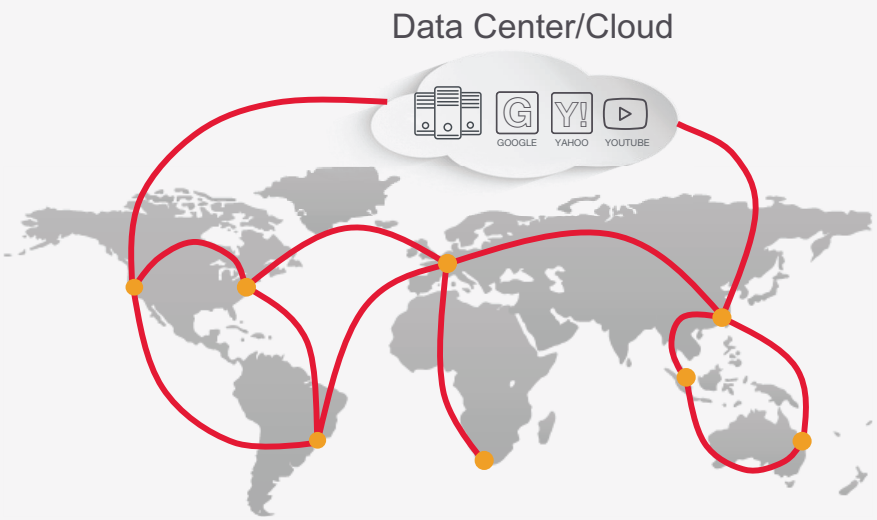
APM solutions can also help with compliance on SLAs. Business rules can be set to alert an administrator when there is a problem to ensure that business-critical applications and functions receive priority. It is even possible to flag critical transactions and application performance to get information about error rates and response times. Some solutions also allow you to visualize performance metrics.

Proactive Monitoring Creates Better and Faster Network Rollouts

Summary

- End users detect and report many network problems.
- Proactively generate network traffic to test SLAs for on-premises and cloud networks.
- Pretest how an application will perform on the network under load before your users do to create faster and better network upgrade rollouts.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Proactive monitoring uses visibility technology to actively test your network. Unfortunately, it is end users who end up detecting and reporting many network problems. This is where proactive troubleshooting can help.

Proactive monitoring has several fundamental benefits, including the ability to

- know immediately what the performance level of your network is
- understand how well your applications are running
- validate SLAs — both on-premises and in the cloud
- test upgrades during maintenance windows before company employees do

Network performance and application performance may sound simple, but these can be difficult to ascertain. To get a true indication of network performance, the network needs to have a large amount of traffic on it, which makes you dependent upon peak busy hours. This solution allows you to place probes anywhere in your network and test whenever you want to. It also allows you to accurately simulate the right traffic so that APM tools can observe how well applications are truly performing. For instance, this allows you to simulate small packets or Skype-like data to test your instant message/voice/video solution.

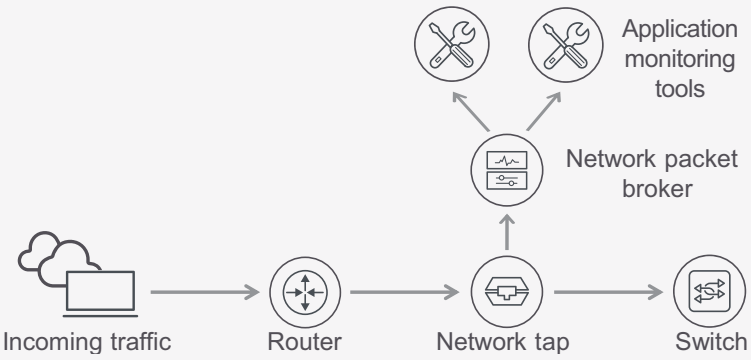
SLA validation can happen during business hours, since it does not disrupt service. This enables you to validate the SLA performance at will. You can then use the information gathered to inform management about which goals were met. If the goals are not met, you can use the impartial data you have collected to contact your vendor and request a fix for any observed network problems or a discount if the vendor fails to meet agreed-upon SLAs.

Optimize Network Performance Monitoring Effectiveness

Summary

- Use an NPB to deliver all required traffic from anywhere in the network to the network performance monitoring (NPM) tool to record 100% of the traffic for playback and analysis.
- Support all network speeds (1G, 10G, 40G, 100G) or virtualized data ports with your existing NPM tool(s).
- Analyze the captured traffic for anomalies and quick problem resolution.

Deployment scenario: Out-of-band visibility architecture



Solution overview

NPM tools can be highly effective in diagnosing network issues. These software-based tools can take metrics from your baseline analysis, flow data, and information that comes directly from your network devices to offer a complete picture of your network. However, standalone deployments of these tools may run into problems such as, overloaded disk space and processing, the need for different interface ports based upon network traffic speed, and multiple input ports to capture data across the network. An NPB can capture network monitoring data and filter that data before it goes to the NPM tool. This process increases the efficiency of the tool by reducing clutter. The additional removal of duplicate data further enhances the efficiency and eliminates the waste associated with storing irrelevant data. Combining an NPM with a virtual tap and NPB also lets you use physical tools to analyze virtual data to increase the efficiency of your NPM solution. In fact, an NPB can deliver the following benefits:

- aggregates data feeds from multiple sources (taps, SPAN ports, virtual taps, and data switches) and combines the information into a single data stream to the NPM tool
- remove duplicate traffic to save tool disk space and processing resources
- remove out uninteresting data to the NPM tool to make it more efficient

- detects whether the NPM tool is off-line and immediately redirects traffic to another NPM tool on the network to provide redundancy or high availability
- captures and records all traffic data as needed
- provides load balancing of traffic across multiple NPM input ports to provide n+1 redundancy and spread higher data rate traffic across lower rate input ports on the NPM tool

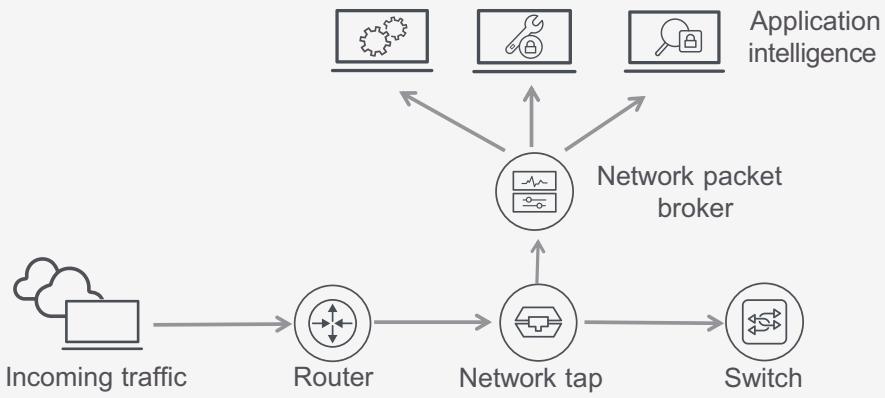
NPM tools and a visibility architecture can help you to stop missing critical network events. The tools help you to essentially rewind your network data and quickly troubleshoot sporadic performance problems. The NPM tools can also navigate to the precise moment a problem occurred to show a detailed before, during, and after packet-level view.

Prevent Application Bandwidth Overloads on Your Network

Summary

- Use an NPB with application intelligence to better understand application and geographic uses of your network.
- Predict application explosions before they bring the network down.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Application intelligence information can predict user and application performance so that you can see whether there are any bandwidth bursts or explosions. For example, consider the case of a mobile carrier that introduced a new smartphone application a few years ago. In a matter of weeks, the interactive app became so popular that usage and bandwidth consumption spiked, resulting in a crash of the mobile carrier's network which lasted for several hours — all because of one application.

The outage resulted in a loss of revenue and public embarrassment for the service provider, as the media got wind of the incident. Had the carrier used application intelligence, the

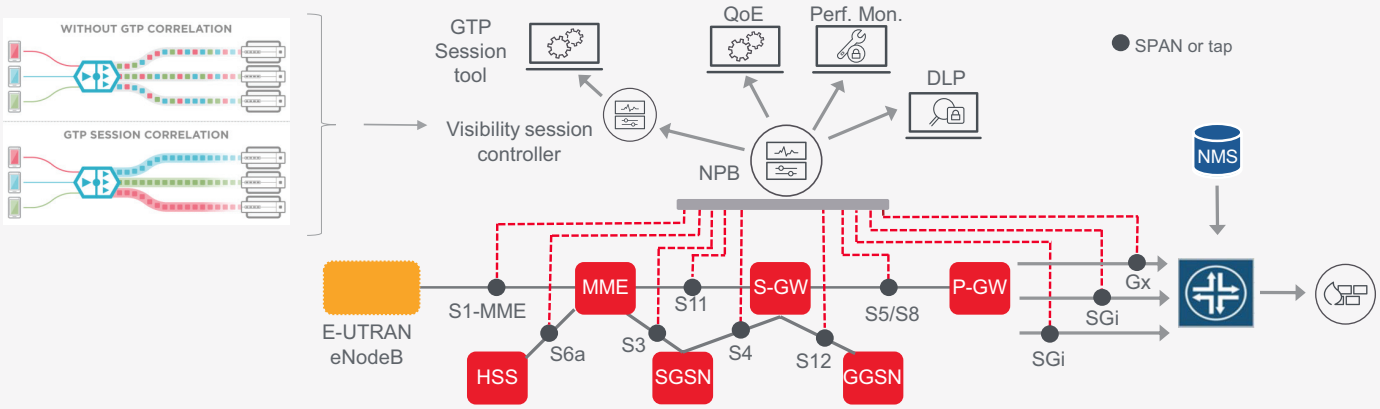
bandwidth consumption of resources by specific applications would have shown up on the dashboard. The system administrator could have easily seen the explosion of bandwidth in real time. Armed with that information, the administrator could then have put controls in place which would have prevented the network outage.

Use a GTP Session Controller to Improve Carrier Customer QoE

Summary

- Improve network service dependability and customer QoE.
- Enable monitoring solutions to scale by offloading the correlation of subscriber data from monitoring probes to a GTP session controller.
- Sample and segment GTP sessions to reduce traffic directed to probes.
- Automatically detect probe failure and redistribute traffic until the probe recovers.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Mobile carriers continually look to improve network service dependability and their customers' QoE; this effort typically leads to higher levels of service assurance and increased revenue. Service providers, especially wireless service providers, need good customer problem data on things like service holes, malfunctioning radios, poor coverage, and even customer dissatisfaction, in order to plan their networks and deliver a better QoE. An important element in this process is the use of sophisticated and costly network monitoring probes that allow mobile carriers to immediately detect and resolve issues that impact QoE.

While network probes can provide visibility into wireless core networks, these devices have limited capacity and may not withstand fluctuating mobile subscriber traffic. At the same time, the under-loading of network probes can create additional costs for the carrier.

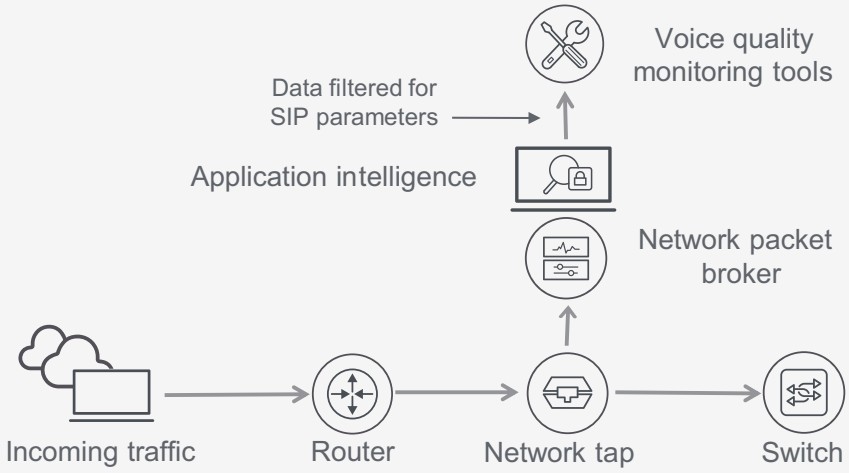
A GTP session controller can effectively identify and track mobile subscribers. At the same time, it also correlates data from network probes which can load balance bandwidth to enforce capacity and rate limits for each customer, even as mobile traffic rates fluctuate. If the controller detects faulty or overloaded monitoring probes, it automatically redistributes the load to other probes in the cluster. As a result, monitoring probes can focus on QoE analysis, rather than spend cycles trying to reassemble GTP session traffic. This allows you to maximize network probe capacity while improving visibility into the wireless core network.

Improve and Simplify Voice Quality Monitoring Efforts

Summary

- Many IT personnel spend over 50% of their time working on network and application performance problems.
- Web conferencing companies can use an NPB with application intelligence to better segment monitoring data since they have separate tools for carrier and native voice over internet protocol VoIP.
- Application sub-definition information, such as Session Initiation Protocol (SIP) and codec field, makes intelligent routing decisions for monitoring data possible.

Deployment scenario: Out-of-band visibility architecture



Solution overview

In addition to being able to detect application definitions running on a network, a proper application intelligence solution needs to capture and distinguish application sub-functionality as well. This provides even more context-aware data processing capabilities.

For example, some SIP-based voice quality monitoring solutions need to understand whether the voice source is a traditional voice call or a digitally generated, voice over

IP using a computer, call. They cannot simply filter monitoring data based upon SIP because all the connections are SIP at the monitoring point. Fortunately, SIP has a codec field that indicates the voice source. An NPB with data processing capability can read the codec field to understand the different source media types and pass that information along to the right type of voice quality tool for proper analysis. The NPB can then send calls from different sources out different NPB ports to the appropriate monitoring tools.

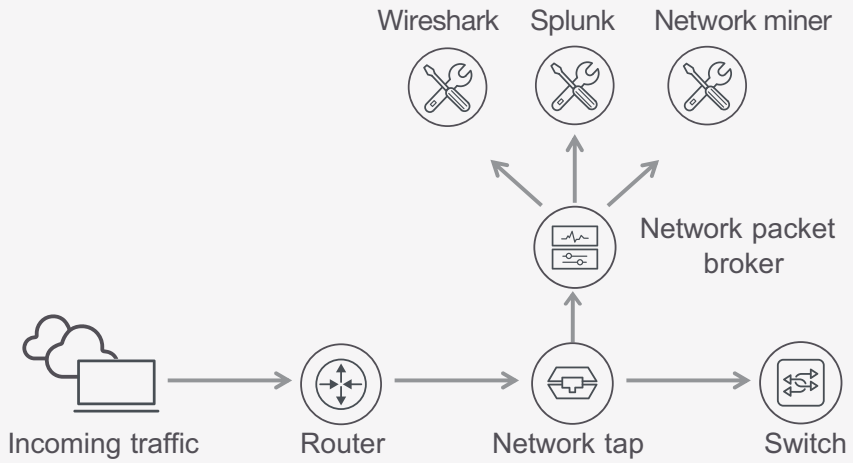
Information granularity like this reduces application troubleshooting costs and allows you to optimize customer quality of experience by providing the all-important details. It is one thing to know that something is happening, it is another to know why.

Focused Deep Packet Inspection Optimizes Your Network Data

Summary

- Use of DPI can increase network performance and security.
- NPBs with application intelligence can capture key information for data mining.

Deployment scenario: Out-of-band visibility architecture



Solution overview

DPI is a general term for gathering extensive information from packet capture and analysis. DPI looks at not only the packet header, but the data part of a packet to gather information. The use of this data can improve network management, network security, and data mining. Examples include finding indicators of compromise, fault isolation, performance impairments, compliance/policy issues, and the ability to offer new services like usage-based billing or advice-based billing.

You can realize additional benefits by using flow-based data to break down traffic metrics inside the network so that you can see, via a flow graph, exactly where all the traffic flows.

Depending on how you configure this protocol, you can break down this information into IP protocols, user datagram protocol (UDP) ports, and even user IDs or IP addresses.

There are essentially three levels of packet inspection:

- deep packet capture
- focused deep packet captures for events like security review
- deep packet inspection of the data portion of the packet

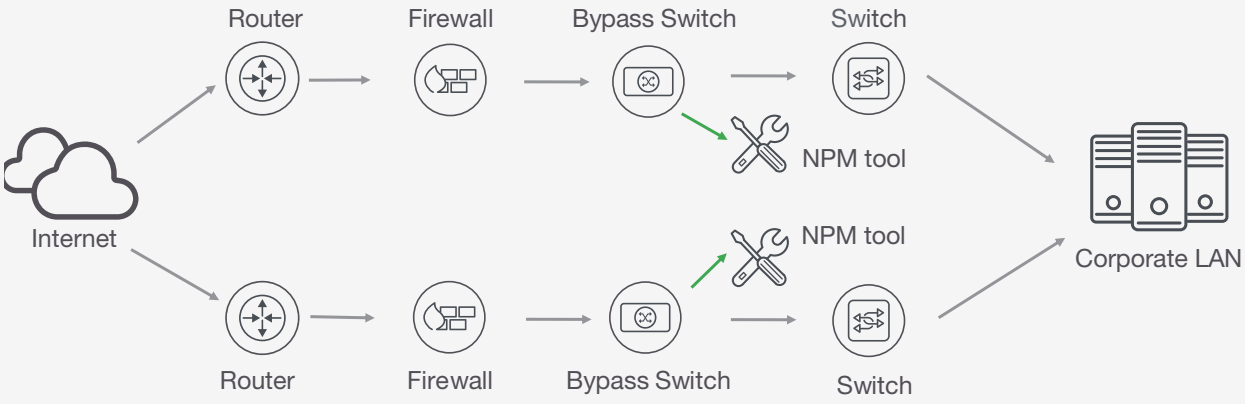
An NPB can segment the data as needed based on specified criteria to look at almost any inspection parameter; this commonly includes Layer 2 through 4 information. Application intelligence functionality with the NPB can provide Layer 7 data as well. This data is then sent to various tools like Wireshark for packet capture analysis, NetworkMiner (a network forensic analysis tool that helps enforce policies and reconstruct events), The Dude (a network monitoring tool that monitors devices and offers alerts when there is a problem), Splunk (a data collection and analysis platform for items like event logs, devices, services, and TCP / UDP traffic), and other tools on the market.

Conduct Inline Network Performance Monitoring

Summary

- Capture real-time network performance data to isolate real-time data delivery problems.
- Use inline bypass switches and an NPB to deploy NPM tools that help maximize network performance.

Deployment scenario: Out-of-band visibility architecture



Solution overview

Most use cases for inline visibility are security-related but some, like load balancing and NPM, are not. By deploying NPM solutions inline, the IT engineer can get immediate access to network activity, such as bandwidth use, flow volume, application response times, and key network events.

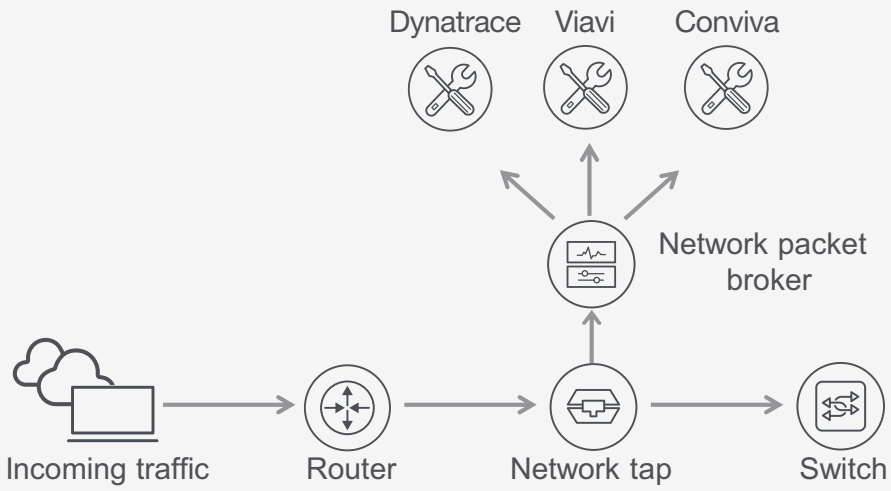
One use case for deploying an inline NPM solution involves understanding deployment differences for the corporate data backbone. This is a common use case for banking and financial trading organizations. For instance, if you have a dual core backbone deployed for redundant load sharing and notice performance differences between the two networks, (data arrives faster on one network versus the other), the inline NPM solution will allow you to characterize both networks to isolate transmission speed differences. This happens by inserting a bypass switch into each network and then connecting both bypass switches to an NPM tool. The NPM can then analyze both networks in real-time to characterize the source of the problem(s).

Better Data Collection Makes QoE Monitoring More Effective

Summary

- Understanding how to use QoE monitoring can be a competitive differentiator.
- Many organizations use NPBs to increase user satisfaction.
- NPBs paired with application intelligence can capture key information for data analysis.

Deployment scenario: Out-of-band visibility architecture



Solution overview

QoE is a measure of the overall level of satisfaction with an application, connection, and speeds. QoE differs from quality of service (QoS), which embodies the notion that hardware and software characteristics can be measured, improved, and perhaps guaranteed, leading to network reliability and performance. QoE measures customer satisfaction, failed customer interactions, design flows (like user navigation across a website), and data that marketing teams can potentially use to optimize customer experiences on websites, portals, and more.

This data can enable businesses within industry segments, like healthcare, media, and financial trading organizations to understand how customers are, and are not, using the business' website and services. Do problems and delays exist? If abandonment occurs, at what juncture? And what was happening at the time? Organizations want to know ahead of time, not when a customer submits an urgent support request or calls to complain about a problem.

An NPB with application intelligence can segment certain criteria parameters like protocols (RTP packets), application-level information (application type, application availability, and application sub-functions used), and data from specific locations like virtual local area

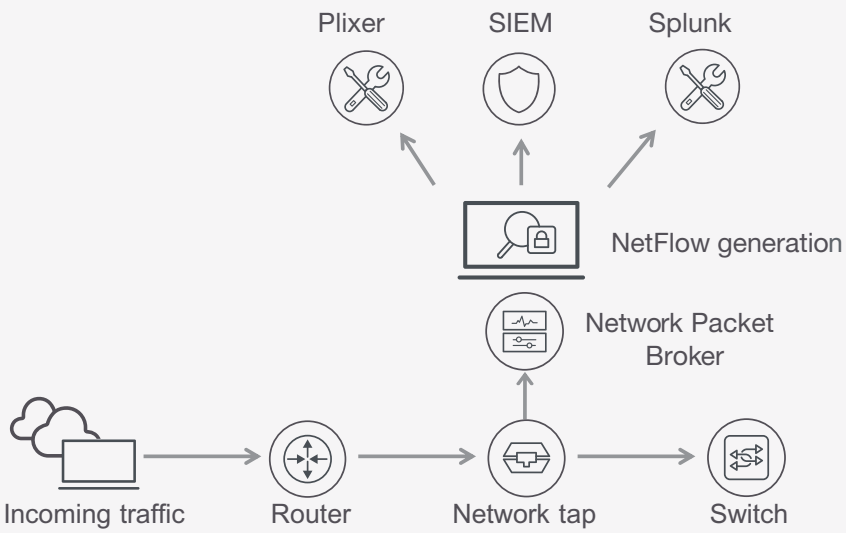
networks. This data can feed specialized tools for analysis such as Dynatrace tools that are used for application monitoring to diagnose Web user navigation experiences, Conviva, which monitors player satisfaction monitoring, and Viavi that monitors customer interaction experiences.

Offload NetFlow Data Generation to Improve Switch Performance

Summary

- Many organizations use network flow data for advanced analytics.
- NetFlow data provides summarized information on traffic applications and patterns for network optimization.
- NPBs can generate NetFlow data and send to a NetFlow collector.

Deployment scenario: Out-of-band visibility architecture



Solution overview

NetFlow, a Cisco protocol, was developed 20 years ago to help IT engineers gain insight into networks. Detailed packet captures are often the best source of insight because they contain payload information. However, increasing network speeds and the effort needed for packet captures is making flow data even more useful. Instead of capturing origination, destination, ports, and protocols for one data stream, NetFlow, and the Internet Engineering Task Force (IETF) version called IP Flow Information Export (IPFIX), aggregates this information for multiple data streams to illustrate activity across the network. This information enables IT engineers to view resource usage across the network, improve troubleshooting, capture signs of unauthorized traffic, data exfiltration, validate QoS parameters, expose denial-of- service attacks, and much more.

However, there are some issues associated with NetFlow:

- Older Cisco switches cannot generate this data.
- Newer Cisco switches can become taxed if the feature is turned on.
- Cisco is the only network switch vendor that generates this data.

Luckily, adding an NPB to your network can overcome these issues. The NPB can generate NetFlow data and send that data to a NetFlow collector, such as a security information and event management tool (SIEM), a Plixer device, or Splunk device. For example, one of the main issues with NetFlow/IPFIX is that it may burden the routing switch during periods of high usage. As the CPU for the routing switch reaches maximum capacity, it will start to shed load, which may impact NetFlow data resulting in slow response times or gaps in data capture. An NPB that supports NetFlow can offload this function from the routing switches. When combined with context-aware data processing, the NPB can deliver application intelligence far beyond what the Cisco switch delivered natively.

Conclusion

The fastest, and often best, 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 data flows. Ultimately, this allows you to identify potential problems and the solutions to improve network performance.

A visibility architecture offers access to additional forms of data that can help improve performance monitoring activity and

- capture performance-related data as quickly as possible which is also the best quality data possible
- capture the right types of data and distribute it to your monitoring tools
- harness the power of application intelligence to improve the quality and speed of your monitoring and analysis activities

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