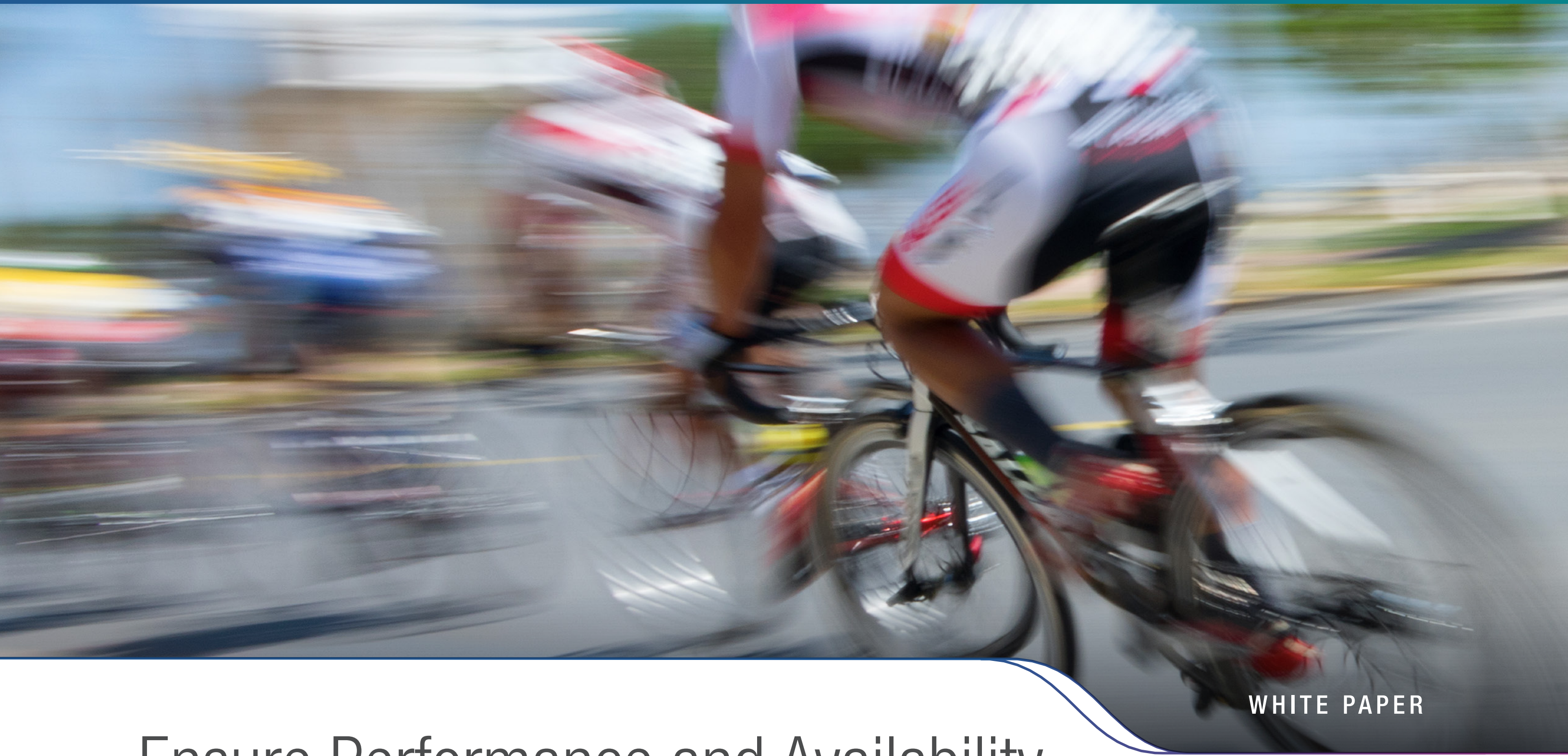


WHITE PAPER

Ensure Performance and Availability of Business-Critical Applications

Introduction

We live in a world of fast information access, powerful applications, and customized user experiences. Services and applications that were not even possible a decade ago dominate our professional and personal lives. If you are responsible for deploying and managing a network, you know how critical network performance and availability are to the delivery and consumption of our most valuable applications and services.

Numerous network issues can affect application performance. The launch of a service or application can stress parts of the network not yet ready to handle the volume. The use of cloud resources can make it difficult to monitor traffic entering or leaving your network. A distributed denial-of-service (DDoS) attack can bring down the infrastructure responsible for revenue generation and affect the bottom line.

What network operations engineers need is better, faster, and more detailed network intelligence. With the right data, you can ensure that your network is able to deliver applications and services with the expected level of performance and respond effectively to a security attack. This paper explores how information collected from your network helps achieve these goals.

Information collected from your network helps you deliver consistent application performance and ensure an excellent user experience.

Packets: The Source Of Network Intelligence

The first step in identifying a potential network issue is to know what is happening across the network. Some issues reveal themselves immediately by affecting large segments of traffic. Other issues take longer to identify because they affect a smaller subset. In the case of a security attack, a single packet might contain the malware or injection responsible for disrupting critical business applications.

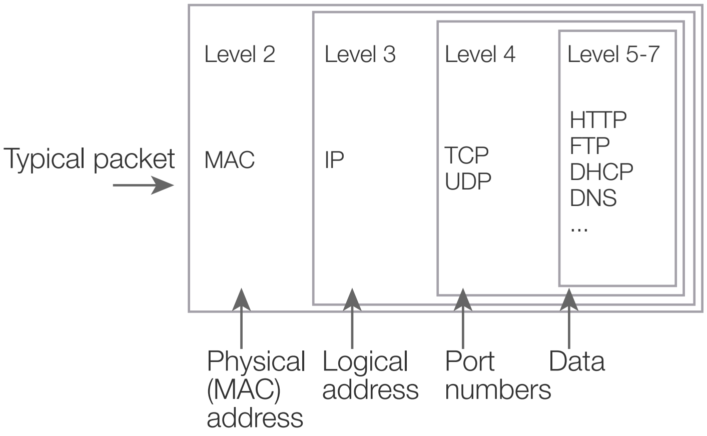
Network packets are the building blocks of digital communications. Multiple headers wrap the payload of a network packet to facilitate delivery to the right location, as shown in Figure 1. Other headers ensure secure delivery of the packet or move it more efficiently to its intended destination. Metadata embedded in the packet provides useful context such as the source, format, purpose, and destination of the packet.

> Network packets are the building blocks of digital communications. Understanding a packet's journey through the network is the source of network intelligence.

Some monitoring tools identify issues by looking at summarized metadata from a group of network packets. Standard firewalls read only the labels or headers on network packets. Other tools , such as application performance monitoring (APM) tools, may require a deeper look into specific packet headers or even the payload of a packet. Tools that perform deep packet inspection, such as forensics analysis tools, analyze packets to reveal which hosts were compromised, what data was affected, and what happened next.

Having direct access to copies of all the packets flowing through the network gives IT teams maximum flexibility in problem-solving. Many experts consider packets "the gold standard" for network monitoring.

Diagram of IP Packet with Headers



Packet metadata provides:

- Geolocation of packet source
- Time stamp
- Application
- Endpoint device
- Operating system
- Subscriber indentifier

Figure 1. Packet metadata is the basis of network intelligence

Packet access is therefore fundamental to monitoring the ongoing security and performance of business applications and services. Is there anything you can do to identify a potential issue before you deploy an application on your network? This is the subject of the next section.

Develop Network Intelligence Before Deployment

You can substantially reduce the risk of network disruption or application downtime by validating that your network infrastructure can support a new workload before you move it into production. This is particularly true in situations where:

- users will access the application via wireless networks
- the application will run on geographically dispersed or public cloud resources in a hybrid IT environment
- thousands of users located a significant distance from where the application is hosted will access it

Active monitoring lets you inject simulated application traffic into the live network and observe a realistic user experience.

Poor application performance can disappoint customers, affect reputation, alarm executives, and result in costly and avoidable emergency fixes. To prevent this situation, you can collect quantitative intelligence on network and application performance before production rollout using a network monitoring platform. The data you gather will indicate whether you need to reinforce or upgrade the network to support the expected volume of traffic and users. These assessments reduce uncertainty and help ensure that IT issues do not impact the success of new applications.

Role Of An Active Monitoring Platform

Your team can validate network performance before application deployment using an active monitoring platform to test your production network. “Active” refers to the approach you use to identify performance issues. You do not just wait passively for live traffic or users to tell you what is going wrong on the network. Instead, you are actively testing the network to find and address any weaknesses that might degrade or disrupt application performance.

In active monitoring, you compose highly realistic test scenarios using a mix of applications that typically flow on your network at volumes you might expect during heavy traffic periods. The integrated platform gives you the ability to generate test traffic and to measure and track key performance indicators. The dashboard flags any results that do not meet threshold expectations, so you can fine-tune or upgrade your infrastructure before deployment. Pre-deployment assessments are particularly valuable in the following common use cases.

Pre-Deployment Application Testing

Validate cloud architecture. Cloud resources offer unparalleled agility, elasticity, and cost benefits. However, migration has one noteworthy drawback: application traffic travels at least partially over the internet, rather than solely on infrastructure you control. While controlled environments on-premises offer stability, the internet is less predictable — leaving your applications vulnerable to latency issues. You can reduce the risk that cloud deployment will degrade application performance by running simulated traffic over your cloud or hybrid architecture and measuring key performance indicators.

Validate user experience. Performance of the physical and virtual infrastructure you use to run an application or service affects your users' experience. This infrastructure may include a combination of endpoints (such as laptops and mobile phones), distributed resources (such as branch/remote office routers and applications), and data center resources (such as servers and databases). To gather data on the end-user experience, you can test the entire infrastructure chain using simulated traffic.

Creating realistic test traffic to measure performance is easier when you have access to a library of common application signatures and a platform to automatically generate the traffic. With manual programming eliminated, you can quickly create and run a simulation using the same applications running on your network. A key feature of active monitoring platforms is the breadth of their application library. Another important feature is the ability to measure response time on a wide range of potential endpoints in the network, including multivendor equipment and various service provider networks, as shown in Figure 2.

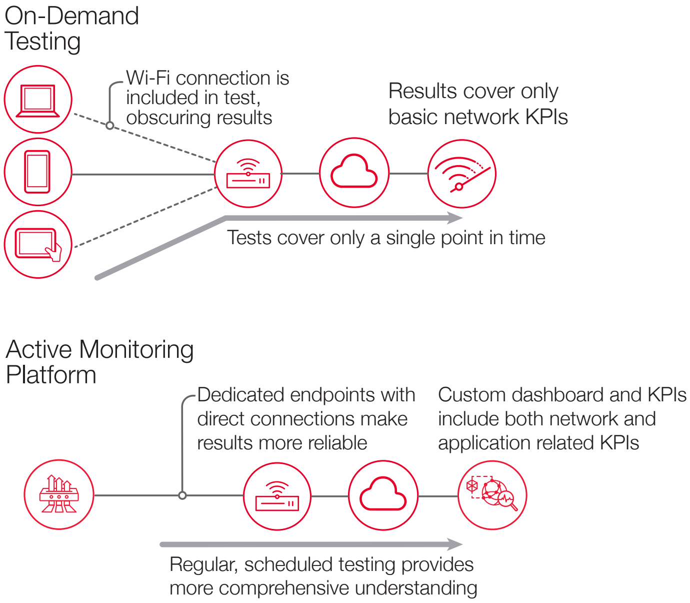

On-Demand Testing
Wi-Fi connection is included in test, obscuring results
Results cover only basic network KPIs
Tests cover only a single point in time
Active Monitoring Platform
Dedicated endpoints with direct connections make results more reliable
Custom dashboard and KPIs include both network and application related KPIs
Regular, scheduled testing provides more comprehensive understanding

Figure 2. Differences between web based testing and active monitoring platform.

Test performance under stress. Developers test and measure application performance in the lab, but that is not the same as observing what happens to an application or service under real-world conditions. New services often work well during the rollout period when fewer users are active, but subsequently suffer outages or performance degradations as usage increases. Active monitoring lets you see exactly what happens to response times when traffic reaches the expected volume or scales up during a seasonal surge.

Continuous monitoring is your first line of defense against application outages and disruption.

Test your security architecture. One of the biggest threats to application performance comes from cyberattacks that overwhelm or disrupt the normal operation of your infrastructure. Organizations rely on a variety of security solutions to protect their networks from attacks and malware. But the more tools deployed, the more complex a security infrastructure becomes. It can be difficult to verify that your security solutions are working.

A security testing platform lets you process application test traffic embedded with DDoS attacks, exploits, and malware through your security architecture. The test reveals how your security solutions protect you against active threats. If your solutions fail, you can use that information to address any security gaps and strengthen your network.

Gather Performance Data Continuously in Production

Once you move applications into production, continuous performance monitoring is your first line of defense against disruption. The right information can alert you to an impending problem and let you make changes before services start suffering. Consider the following strategies:

Deploy your monitoring architecture up front. Maintaining application performance will be faster and easier if you deploy monitoring solutions alongside your infrastructure. Determine how you will access packet data from each segment of your network. Taps generally provide a more robust solution than the switch port analyzer (SPAN) ports on your network switches. Taps require little to no configuration and are not IP addressable, so they are not vulnerable to outside attack. Taps do not introduce delay or alter the content of the network packet in any way. You can purchase physical taps for copper, multimode, and single-mode optical fiber at speeds from 1–400 Gbps. Virtual taps that operate within the hypervisor layer provide access to data packets that flow between virtual resources.

Ensure complete packet access, with no blind spots. What does it mean to have a blind spot in your monitoring architecture? Blind spots are areas of your network where data packets are not visible to your performance monitoring and security tools. This happens when you do not monitor enough network segments or do not use the right technology to access data packets in virtual or cloud-based resources. In a hybrid IT environment, you need to supplement your physical taps with virtual taps and container-based cloud sensors to access all your application traffic, *even the packets that move only between virtual resources (known as east-west traffic)*. Complete access is essential because blind spots can hide clues to the cause of an application slowdown or failure. You need all the clues available to identify issues accurately.

Use Packet Processing to Increase Speed and Efficiency of Application Monitoring

Your special-purpose performance monitoring and analysis tools need network packets to identify irregularities and spot vulnerabilities. However, sending all your raw, unfiltered packets to every monitoring tool is inefficient. You need a way to quickly sort through the data and zero in on what is relevant.

A packet broker (or processor) gives you more control over the data you deliver to your application monitoring tools.

Role of a Network Packet Broker

A class of products known as network packet brokers (NPBs) provides the processing power and speed to filter raw packets, identify and condense relevant data, and deliver data to your application monitoring tools at very high speed. You can purchase an NPB as a physical device with customized, high-speed processors or as a service you run on a white-box server.

NPBs are deployed between your data access devices (taps and SPAN ports) and your monitoring tools, as shown in Figure 3. An NPB time-stamps each packet and recognizes details such as the sender's IP address, endpoint device, operating system, and the application in use. Vendors call this "context awareness," and it gives you more control over the data you send to your tools. You configure data filters on an NPB using a simple graphical drag-and-drop interface. You can easily sort through packets to isolate those with specific characteristics. NPBs provide you with:

- better data for better decisions
- stronger security
- faster problem resolution
- deeper intelligence
- increased efficiency of monitoring tools

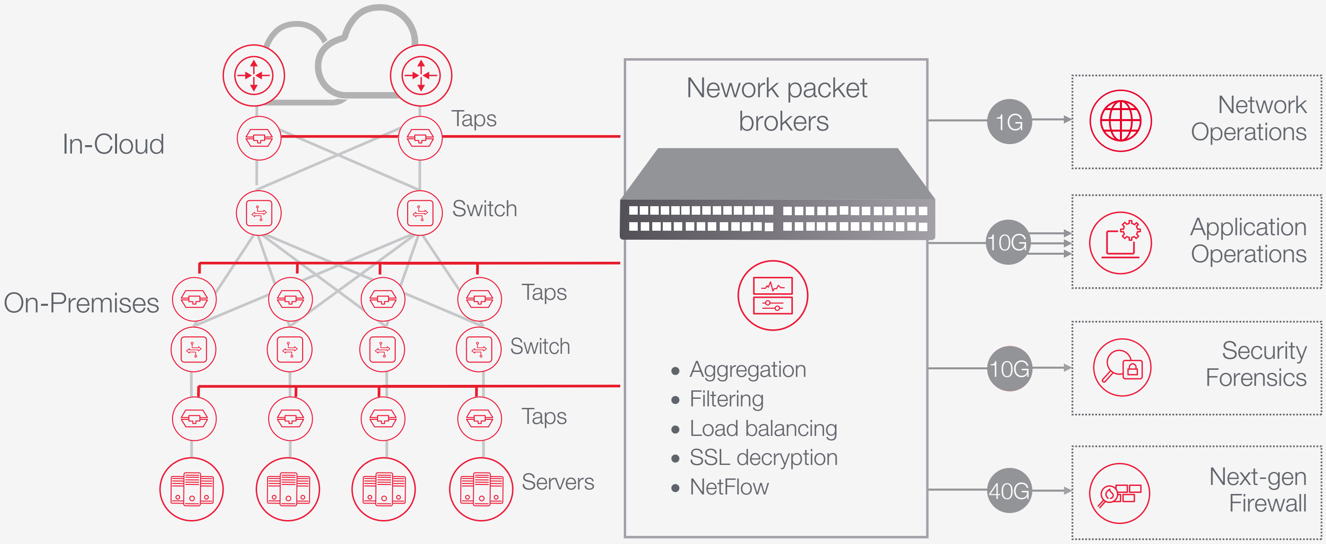


Figure 3. NPBs act as a control layer to make application monitoring easier, faster, and more efficient.

You can improve the speed, cost-efficiency, and accuracy of application monitoring when you use an NPB to do the following:

Aggregate and condense application data flow. Network paths in modern organizations are redundant to ensure reliability. As you collect application data, you will naturally end up with lots of duplicate packets. These duplicate packets can easily double the workload for your monitoring tools, increase costs, and cause tool congestion. When tools become congested and run out of capacity, they drop packets and can produce inaccurate results. An NPB can easily eliminate duplicate packets to reduce the workload on your monitoring tools. It can also strip out packet headers or payloads that your monitoring tools do not require.

Zero in on relevant data. Different monitoring tools require different types of data. With an NPB, you can quickly and automatically sort through the packets you collect to provide specific data to each of your monitoring tools or for specific situations. For example, you may want to find all the traffic associated with a particular application that is running slowly. An NPB can provide your APM solution with exactly that traffic. You can find the root cause of an issue faster and more efficiently.

Adjust data delivery to match tool capacity. Monitoring tools connected directly on the network must operate at the same speed. When you decide to upgrade the speed of your network, you must also upgrade your tools. This increases the cost of an upgrade considerably. If you deploy an NPB control layer between your network equipment and your tools, you can deliver data at any rate you choose. This feature lets you delay purchasing higher-speed monitoring tools.

With an NPB-based control layer, you can filter data packets at high speed, decrypt secure packets, and adjust the speed of delivery to your monitoring tools.

Deliver relevant data to multiple tools. You can set up your NPB to manage the flow of packet data in whatever way makes sense. For instance, you can send a set of data to multiple monitoring tools at the same time, or you can pass data consecutively from one tool to the next, depending on your monitoring results. You specify the path data will take with a graphical, drag-and-drop interface that new employees can use without extensive training.

Monitor secure traffic more efficiently. Senders and receivers commonly use encryption to protect the transmission of sensitive and private communications. Encryption makes it harder for hackers, but it also slows down application monitoring. Decoding encrypted traffic is process-intensive and can quickly use up a tool's capacity. A faster and more cost-efficient approach is to offload decryption from your monitoring tools. An NPB with active SSL decryption can decode secure packets one time and then deliver the resulting plain-text packets to multiple monitoring tools. You save all of the tool's processing capacity for its intended purpose.

Increase the resiliency of application monitoring. An NPB gives you control over data flow, even when one of your monitoring tools fails. If your NPB detects that a monitoring tool is offline for any reason, it can automatically reroute data to another tool to avoid disruption.

Conclusion

You can improve performance and availability of your business-critical applications with Keysight solutions for gathering and filtering network data. The intelligence you develop from your network data supports application performance, from concept to operation. Whether you are preparing to migrate a business-critical application to a hybrid infrastructure, roll out a new service to customers or employees, or simply manage performance in production, Keysight solutions help you reduce the risk that an outage or slow performance will impact your business. The result will be stronger networks, more consistent application performance, and an excellent user experience

Learn more about Keysight's performance monitoring solutions at https://www.keysight.com/my/en/cmp/2020/network-visibility-network-test.html.

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