What Is a Network Packet Broker

(AND WHY DO YOU NEED ONE)?

KEYSIGHT TECHNOLOGIES

Introduction

Keeping networks safe and users thriving amid the relentless flux requires a host of sophisticated tools performing real-time analysis. Your monitoring infrastructure might feature network and application performance monitors, data recorders, and traditional network analyzers. Your defenses might leverage firewalls, intrusion prevention systems (IPS), data loss prevention (DLP), anti-malware, and other point solutions.

However specialized security and monitoring tools may be, they all have two things in common:

- They need to know exactly what is happening in the network
- Their output is only as good as the data they receive

<70%

of network segments are monitored by IT professionals

38%

cited "network complexity" as the main reason they can't monitor 100% of segments[1]

Ideally, a company would monitor 100% of its network with security and monitoring tools. In reality, this is not always the case. A 2018 survey conducted by Enterprise Management Associates (EMA) found that the majority of enterprises monitor less than 70% of their networks.1 When asked why they do not monitor 100% of their networks, the top response (38%) from IT professionals was "network complexity". This feedback equates to having blinds spots in the network, and ultimately, to wasted effort, redundant cost, and a higher risk of being hacked.

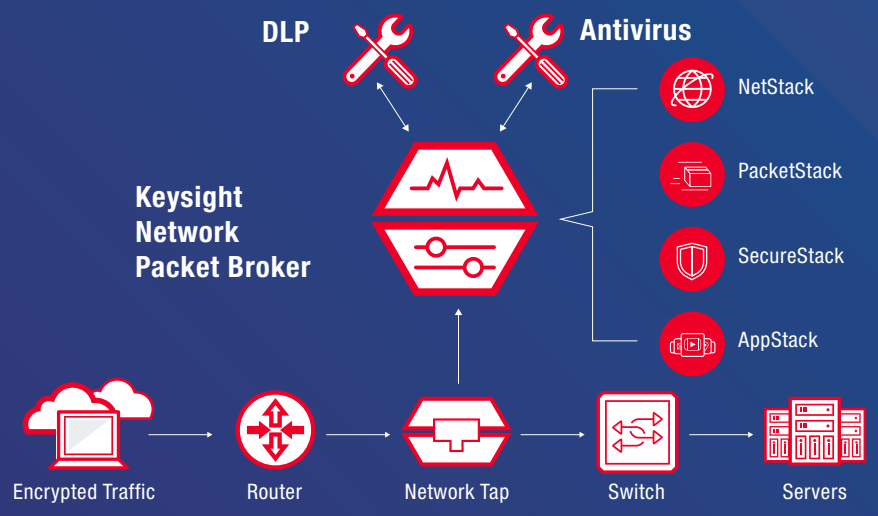
To avoid waste and blind spots, start by collecting data about what is taking place across your network. Network taps and mirror ports on network equipment—also known as switched port analyzer or SPAN ports—create access points for capturing traffic for analysis.

This can be considered the "easy part." The real challenge lies in efficiently funneling data from the network to each tool that needs it. If you only have a few network segments, and relatively few analysis tools, the two may be connected directly. More often, 1:1 connections may pose a management nightmare that becomes unwieldy, if not logistically impossible as the network grows. Additionally, ports on high-end analysis tools, such as firewalls, may also be in even shorter supply, and it is critical not to overtax devices to the point of compromising performance.

"Packet loss in a network visibility tool should be unacceptable. Visibility is supposed to enable clear insight into network data, not degrade the data that the analytics tools require."

TOLLY

[1] McGillicuddy, Shamus. "Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics." Enterprise Management Associates Research, August 2018.



5 ways to improve ROI with packet brokers

- Speed troubleshooting
- Detect breaches faster
- Reduce burden on security tools
- Extend the life of monitoring tools during upgrades
- Streamline regulatory compliance

Why Do I Need a Network Packet Broker?

A Network Packet Broker (NPB) resides between taps and SPAN ports. They can access network data and sophisticated security and monitoring tools that typically reside in data centers. NPB's do just what their name says: they broker network packet data to ensure every analysis tool sees exactly the data it needs to perform at the highest possible level. The NPB adds an increasingly critical layer of intelligence—one that reduces cost and complexity to help you achieve the following:

Better data for better decisions

A fabric of packet brokers with advanced filtering capabilities serves to organize and streamline data for your monitoring, performance, and security tools.

Tighter security

It is hard to stop threats when you do not see them coming. NPBs work to assure that your firewalls, IPSs, and other defenses see exactly the right data, all of the time.

Faster problem resolution

Zeus Kerravala, principal analyst at ZK Research, observes, "Problem identification is IT's biggest challenge." Identifying that there is, in fact, an issue consumes up to 85% of mean time to repair (MTTR). Downtime is money

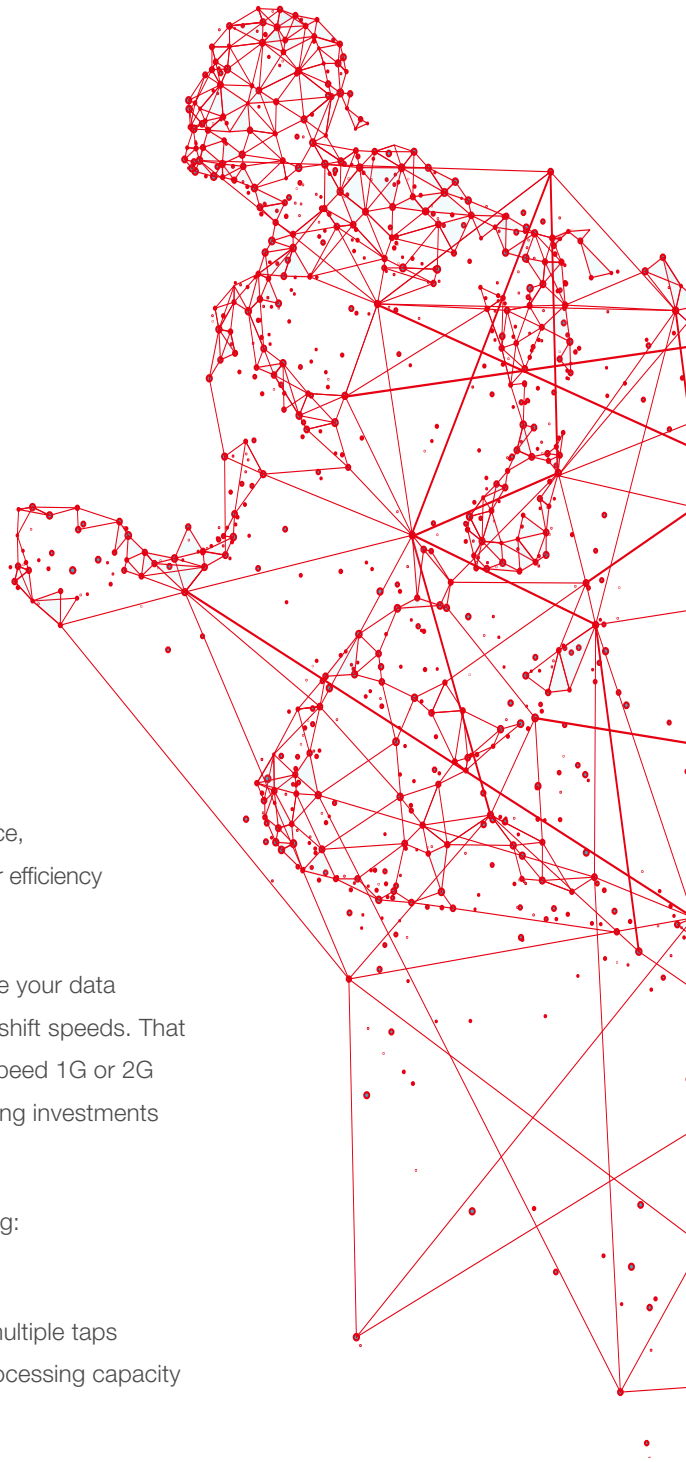
Context-aware filtering provided by NPBs helps you detect and determine the root cause of issues faster by introducing advanced application intelligence. Ixia's robust Security Fabric leverages this intelligence to speed up troubleshooting by providing insight into the geographic location of outages and the vendors that may be causing disruptions.

Increased proactivity

The use of metadata, provided through NetFlow by intelligent NPBs, also aids in accessing the empirical data used to manage bandwidth usage, trending, and growth. That prevents problems from occurring in the first place.

Better return on investment (ROI)

Intelligent NPBs do not merely aggregate traffic from monitoring points the way a switch might. They filter and groom data to enhance the utilization and productivity of security and monitoring tools. With only relevant traffic to process, they help improve tool performance, reduce congestion, minimize false positives, and achieve better coverage using fewer devices.



What Exactly Does the NPB Do?

Conceptually, aggregating, filtering, and delivering data sounds simple. In practice, intelligent NPBs perform sophisticated functions to produce exponentially higher efficiency and security gains.

One way they do this is by load balancing traffic. For example, if you upgrade your data center network from 1Gbps to 10Gbps, 40Gbps, or higher, NPBs can downshift speeds. That allows you to distribute higher speed traffic across a pool of existing lower-speed 1G or 2G monitoring tools for analysis. This extends the value of your existing monitoring investments and avoids costly rip-and-replace upgrades as you migrate.

Other powerful features and functions the NPB performs include the following:

Deduplicating redundant packets

Analysis and security tools stand to receive a slew of duplicate packets as multiple taps forward traffic. NPBs can eliminate duplicates to keep tools from wasting processing capacity by handling redundant data.

SSL decryption

Secure Socket Layer (SSL) encryption is the standard technology used to safely send private information. However, hackers can hide cyberthreats in encrypted packets.

Decryption is necessary to inspect this data, but unraveling code takes valuable processing power. Leading packet brokers can offload decryption from security tools to ensure total visibility while easing the burden on high-cost resources.

Data masking

SSL decryption leaves data visible to anyone with access to security and monitoring tools. NPBs can mask personally identifiable information such as credit card and Social Security numbers, protected health information, and other sensitive data, before passing it on. That means tools and their administrators cannot see it.

Protocol header stripping

An NPB may strip out protocol headers such as VLAN, VXLAN, and L3VPN, allowing tools that process these protocols to receive and process packet data. Context-aware visibility helps in spotting rogue applications running on your network and footprints attackers leave as they work their way through your systems and networks.

What to look for in an NPB

- Ease-of-use and management
- Intelligence capabilities that remove the burden from your teams
- No dropped packets – 100% reliability while running advanced features
- Architected for high performance

Application and threat intelligence

Early detection of breaches mitigates the loss of sensitive information and the ultimate cost. Context-aware visibility that NPBs deliver can expose indicators of compromise, identify the geolocation of attack vectors, and combat encrypted threats.

Application intelligence extends beyond Layers 2 through 4 (of the OSI model) to Layer 7 (the application layer) of the packet data. Creating and exporting rich data about the behavior and location of users and applications helps thwart application-layer attacks featuring malicious code masquerading as normal data and valid client requests.

Application monitoring

Application-aware visibility also has profound implications for performance and management. Maybe you would like to know when employees are using cloud-based services such as Dropbox, or web-based email to bypass security policies and transfer company files. Perhaps former employees are attempting to access files using personal cloud-based storage services.

Network Monitoring Tools Face Off

" Using [other vendor's] filters we spent the better part of four hours and some trial and error to get the map and its filters defined and applied. Keysight's smart filtering feature, on the other hand, took all of 10 minutes to perform the same task in our tests."

Bruce Boardman, Network Computing editor

Top Three Considerations in Choosing the Right NPB

Assuming the benefits of using NPBs speak for themselves, remember that not all solutions are created equal. Every network visibility solution is different, and the differences may directly impact the security, cost, and efficiency benefits you achieve. Replicating your unique network environment and conducting a head-tohead bake-off is the best way to put competing solutions to the test. Before you do that, you can use three key selection criteria to thin the field:

Does it perform as advertised—at all times and at any speed?

According to Cisco, global Internet Protocol (IP) traffic levels will more than triple from 1.5 ZB per year in 2017 to 4.8 ZB per year in 2022.[2] Network visibility, and networks themselves, will be hard-pressed to keep up.

Since partial visibility may effectively be the equivalent of no visibility at all, you need to look for a zero-loss NPB solution that can perform advanced functions at the vendor's specified line rate. Keysight builds NPBs for performance, architecting them from the ground up to deliver 100% reliable data processing while performing intelligent filtering, deduplication, SSL decryption, and other processing-intensive functions.

Make sure to assess performance at a load of 60% or higher. A test conducted by Tolly validated that Keysight NPBs processed 100% of the traffic at every speed while running the most advanced features.

By contrast, a competing solution demonstrated packet loss ranging from 20% to nearly 75% at every data size. Worse still, the fact that it had dropped data went unreported.

[2] "Cisco Visual Networking Index: Forecast and Trends, 2017-2022," Cisco, 2019.

How robust is the solution architecture?

Purpose-built to perform intensive processing at line rate, Keysight's network packet brokers are optimized with a field-programmable gate array (FPGA). An FPGA is hardware that accelerates the packet processing engine of the NPB. This design offers significant architectural benefits and delivers full line-rate performance with a single module for better total cost of ownership (TCO) than the competition, which often requires regular investment in additional modules.

Additionally, Keysight NPBs have high-density, modular chassis with customizable bays. This allows enterprises to tailor NPBs to fit their needs, now or in the future, while maintaining a minimal footprint in the data center. Should network requirements change later, modules can be easily switched out to scale as needed. Then, both risks and costs associated with upgrades are minimized while space in the rack is conserved.

Does it enhance your security?

NPBs are the lynchpin of a robust Security Fabric, delivering enhanced resilience along with better threat detection. In typical deployments of two redundant tools, one is generally active while the other exists in "standby" mode for ensured resilience. But, this can mean risking that the standby device has failed silently and will not be available to take over when the time comes.

Keysight NPBs can operate in active-active mode, so both nodes are working, and each is aware of the traffic the other is processing. Should one fail, recovery is instantaneous.

Keysight's solution for large, growing data centers:

Find out more about the Vision X network packet broker.

See for Yourself

Any gap in monitoring or security coverage compromises your ability to manage and defend your data centers, networks, and applications. Contact Keysight or your authorized Keysight reseller to conduct a demonstration tailored to your unique needs and challenges and start seeing better performance, security, and ROI today.

Network Visibility —Performance Matters Video

Network Visibility — Resilience Matters Video

Network Visibility for Dummies Book

Vision X: Scalable visibility for data centers today and tomorrow

Network Visibility — Ease of Use Matters Video

Network Visibility — Feature Compatibility Matters Video

Keysight's 2019 Security Report

5 Ways to Improve ROI with Network Packet Brokers

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

This information is subject to change without notice. © Keysight Technologies, 2019 - 2021, Published in USA, January 12, 2021, 3120-1272.EN