CUBRO
NETWORK VISIBILITY

INTRODUCTORY GUIDE TO NETWORK PACKET BROKERS

WHITE PAPER

MAY 2019

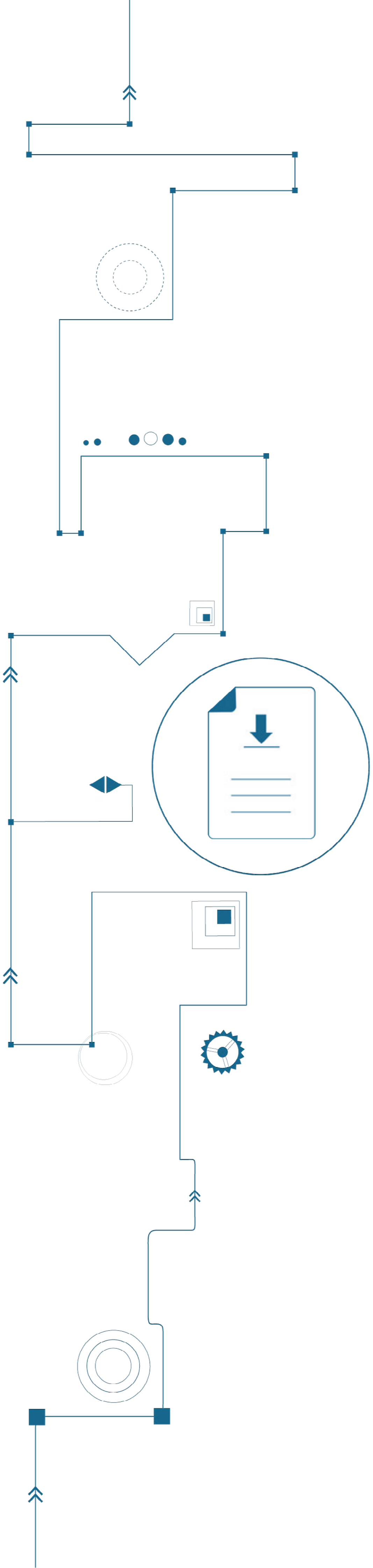

TABLE OF CONTENTS

What is a Network Packet Broker?

A Network Packet Broker (NPB) is a switch-like network device ranging in size from portables devices, to 1 and 2 RU units, up to massive chassis and blade systems. Unlike a switch a Network Packet Broker does not alter the traffic passing through it in any way unless specifically instructed to do so. An NPB can accept traffic on one or more interfaces, perform some pre-defined function on that traffic, and output it to one or more interfaces.

Unlike a switch a Network Packet Broker does not alter the traffic passing through it in any way unless specifically instructed to do so.

This is commonly referred to as “any to any”, “many to any”, and “any to many” port mapping. The functions that can be performed can be as simple as forwarding or dropping traffic and as complex as filtering on Layer 5+ information to identify a specific session. The interfaces on an NPB can be copper connections but are frequently SFP/SFP+ and QSFP cages to allow a broad variety of media and bandwidth speeds to be used. The feature sets of NPBs are built around the principle of maximizing the efficiency of network appliances; particularly monitoring, analysis, and security tools.

What capabilities do Network Packet Brokers offer?

The capabilities of an NPB are numerous and can vary depending on the make and model of the device, though a core set of features are expected of any competent packet broker. The majority of NPBs, thus the ones most frequently encountered, function at OSI Layers 2 - 4.

One critical requirement that a customer should look for in an NPB is that of a non-blocking backplane.

Typically, you can expect to find the following features on an L2-4 NPB: redirection of traffic (or a specific portion of it), traffic filtering, traffic replication, protocol stripping, the ability to slice (truncate) packets, the ability to initiate or terminate various network tunneling protocols, and load balancing of traffic. As might be expected, an L2-4 NPB can filter on VLAN, MPLS tags, MAC address (source and destination), IP Address (source and dest.), TCP and UDP Ports (source and dest.), even TCP flags, as well as ICMP, SCTP, and ARP traffic. This is by no means an exhaustive list of capabilities but should offer an idea of how an NPB operating at Layers 2 - 4 can separate and identify traffic subsets.

A Network Packet Broker needs to be able to support the full traffic throughput of every port on the device; in chassis-based systems the interconnect to the backplane also needs to be able to support the full traffic load of the attached module. Your tools are only as good as the traffic they receive and if the NPBs are dropping packets then the tools do not have a complete picture of the network.

While the vast majority of NPBs are based on ASICs or FPGAs, due to the packet processing performance advantage and their purely deterministic nature, you will find a number that either incorporate or can accept (via modules) CPUs. This is usually to offer features that require flexibility in processing and therefore cannot purely be done in hardware. These features include functions such as packet deduplication, time stamping, SSL/TLS decryption, keyword searching, and regular expression search. There is a caveat with features that depend on CPU horsepower though; the performance of such functions is highly dependent on external variables (e.g. a regex search of the same pattern can net very different performance results depending on the type of traffic, match rate, and bandwidth) and is not easily determined prior to actual implementation. CPU dependent features will be the limiting factor in an NPBs overall performance if they are enabled.

CPUs, along with the advent of programmable switching silicon (e.g. Cavium Xpliant, Barefoot Tofino, Innovium Teralynx), also serve as the basis for the expanded feature sets of the Next Generation Network Packet Broker, units that can handle traffic beyond L4(commonly referred to as L7 Packet Brokers). Of the aforementioned advanced features, keyword and regular expression searches are a great example of Next Gen features. The ability to search the payload of the packet creates the opportunity to filter traffic at the Session and Application Layers and offers far more granular control than L2-4 units can provide to evolving networks.

How does a Network Packet Broker fit into the infrastructure?

A Network Packet Broker can be installed into the network infrastructure in two different ways: inline and out-of-band. Each of these roles offers pros and cons and enables traffic manipulation in ways that the other cannot. Inline, a Network Packet Broker has live network traffic traversing the device en route to its destination. This offers the opportunity to manipulate the traffic in real-time; for instance, duplicating the traffic to a second link while adding, modifying, or removing a VLAN tag or altering the destination IP Address. In an inline role an NPB can also provide redundancy to other inline tools such as an IDS, IPS, or Firewall. The NPB can monitor the status of such a device and, in the case of a failure, dynamically reroute traffic to a hot spare.

In an inline role an NPB can also provide redundancy to other inline tools such as an IDS, IPS, or Firewall. The NPB can monitor the status of such a device and, in the case of a failure, dynamically reroute traffic to a hot spare.

Indeed, a single NPB could handle some traffic links inline while handling other traffic out-of-band simultaneously.

Out-of-band, traffic is copied off of the network via Network TAPs or SPAN/ Mirror ports. This offers a lot of flexibility in how this traffic can be manipulated and replicated to multiple monitoring and security appliances without any impact on the live network. This offers an unprecedented level of network visibility and ensures that all devices receive a copy of the traffic needed to perform their duties properly.

Not only does it ensure that your monitoring, security, and analysis tools get the traffic they need; it can also guarantee that they do not expend resources on traffic that is not needed. Maybe your Network Analyzer doesn't need to record the traffic from your backups, which uses up valuable disk space in the process. Something like that is easily filtered out of the feed to the analyzer while retaining all other traffic to that tool. Perhaps you have an entire subnet that you want to guarantee remains hidden from some other systems; again, this is easily dropped on selected egress ports.

What common problems do Network Packet Brokers solve?

We have already touched on the features and, while doing so, some potential applications for Network Packet Brokers; now let's focus on the most common pain points that NPBs address.

An NPB can accept a traffic feed and duplicate an exact copy of that traffic out to as many tools as the Packet Broker has available ports.

Limited network access for tools:

The number one challenge that Network Packet Brokers address is that of limited access. Put another way, it is the challenge of getting a copy of the network traffic to each and every security and monitoring appliance that needs it. When you turn on a SPAN port, or better, install TAPs in your environment, you have a single source of traffic that probably needs to go to many tools. Furthermore, any given tool should really be receiving traffic from multiple points within the network in order to eliminate blind spots. So how do you get all of that traffic to every tool?

A Network Packet Broker remedies this in two ways: It can accept a traffic feed and duplicate an exact copy of that traffic out to as many tools as the Packet Broker has available ports. Not only that but the NPB can take traffic from multiple sources at separate points in the network and aggregate them together for output to a single tool. Put these two functions together and you can accept all feeds from your SPANs and TAP monitor ports into your NPB, aggregate them as needed and output a copy of that traffic to each and every tool in your environment, all while maintaining granular control of exactly what traffic is sent to each tool. This also includes traffic that a tool may not normally be able to handle.

Network Packet Brokers help you get the most out of your monitoring and security appliances; both from an efficacy and ROI standpoint.

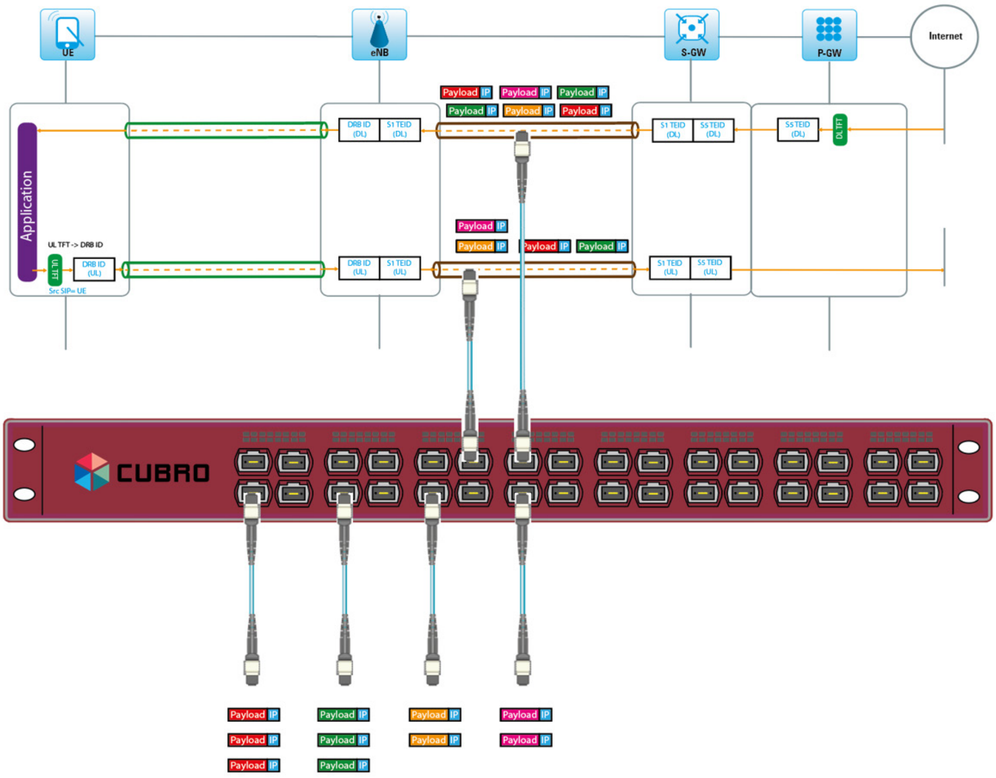

Figure 1GTP Load Balancing

As previously mentioned, it is possible to strip protocols from traffic that may otherwise prevent a tool from interpreting it. The NPB can also terminate tunnels, such as GRE, so that the traffic contained within can be parsed by your various tools.

The Packet Broker also serves as the central hub for adding new tools into the environment. Whether inline or out-of-band, a new appliance can be connected to the NPB and, with a few quick edits to the existing rule table, the new device can be receiving network traffic without any interruption to the rest of the network or any rewiring.

Optimizing tool efficiency:

Network Packet Brokers help you get the most out of your monitoring and security appliances; both from an efficacy and ROI standpoint. Let’s consider a few potential scenarios you may encounter with these tools. It’s fair to say that a lot of your monitoring/security appliances are probably wasting processing power on traffic that is not relevant to that device. Eventually, you will likely get to the point where the device has reached its limitations processing both useful and not so useful traffic. At this point the vendor for that appliance will certainly be happy sell you a beefed-up replacement with even more processing capability to solve your problem...for a time, anyway.

What if we could just get rid of the traffic that is meaningless to the tool in question before it gets there.

Additionally, let’s assume an appliance really only looks at header information for the traffic it receives. Slicing the packet to remove the payload and just forwarding the header info can reduce the traffic load to the tool dramatically; so why wouldn’t we? A Network Packet Broker can do just that; extending the useful service life of your existing tools and reducing the need to upgrade as frequently.

An NPB can effectively act as a speed converter in this scenario and get the traffic to the tool.

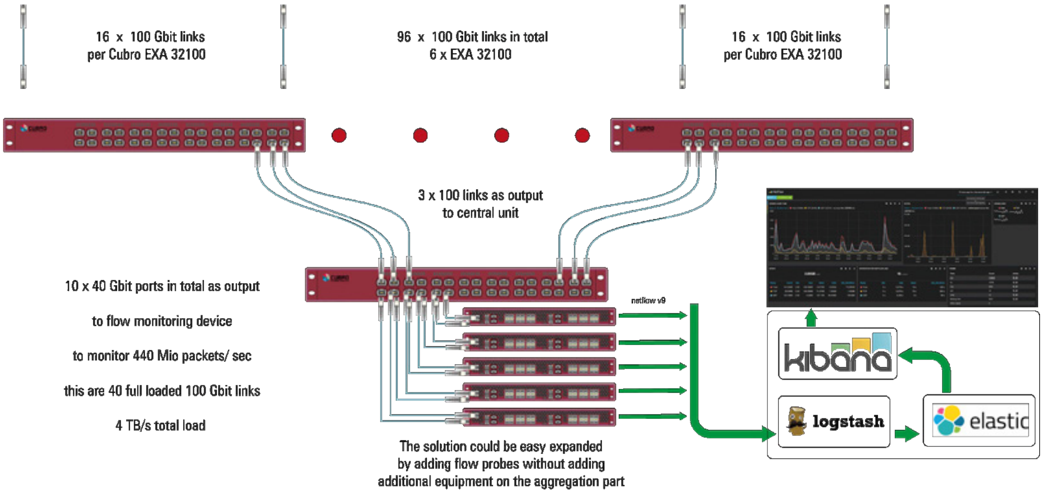
16 x 100 Gbit links
per Cubro EXA 32100
96 x 100 Gbit links in total
6 x EXA 32100
16 x 100 Gbit links
per Cubro EXA 32100
3 x 100 links as output
to central unit
10 x 40 Gbit ports in total as output
to flow monitoring device
to monitor 440 Mio packets/ sec
this are 40 full loaded 100 Gbit links
4 TB/s total load
netflow v9
kibana
logstash
elastic
The solution could be easy expanded
by adding flow probes without adding
additional equipment on the aggregation part

Figure 2 Packet Slicing

You could find yourself in a situation where you have exhausted the available interfaces on a device that may still have plenty of processing overhead available. It could even be that the interfaces aren’t carrying anywhere near their available capacity of traffic.

Aggregation with the NPB will address this. By aggregating the data streams going to your appliance at the NPB you can make the most of each interface that device has to offer; optimizing the bandwidth utilization and freeing up interfaces.

Another similar scenario is one where your network infrastructure has, say, moved to 10G while your appliance only has 1G interfaces. The appliance may still be able to easily process the amount of traffic that is on those links but is simply unable to negotiate the speed of the link. An NPB can effectively act as a speed converter in this scenario and get the traffic to the tool. If bandwidth is becoming a constraint then the NPB can also drop irrelevant traffic, perform packet slicing, and load-balance the remaining traffic across the available interfaces of the tool, once again extending its useful service life.

Similarly, the Network Packet Broker can also serve as a media converter while performing these functions; if an appliance has only copper interfaces but needs to handle traffic from fiber links the NPB is once again able to get the traffic to that appliance by serving as an intermediary.

Maximizing your investment in Security and Monitoring appliances: The preceding examples really build up to the next point. Network Packet Brokers allow an organization to get the maximum benefit from their investments. If you have a TAP infrastructure, then the Packet Broker extends access to the tapped traffic to all devices that require it.

Network Packet Brokers allow an organization to get the maximum benefit from their investments. If you have a TAP infrastructure, then the Packet Broker extends access to the tapped traffic to all devices that require it.

The NPB reduces wasted resources by eliminating irrelevant traffic and offloading various functions from network tools so they can handle the function they were designed for. The Network Packet Broker can be utilized to add an extra level of fault tolerance and even network automation to your environment; increasing responsiveness, reducing down time, and freeing up personnel to focus on other tasks. The increased efficiency brought about by the NPB increases network visibility, reduces CapEx and OpEx, and strengthens your organization’s security posture.

Figure 3 Advanced Network Packet Broker

In this white paper we took broad look at what a Network Packet Broker is, what capabilities should be expected of any viable NPB, how an NPB can be implemented into the network, and the most common problems that they address. This is by no means an exhaustive thesis on Network Packet Brokers but hopefully this helped to clarify any questions or confusion about these devices. Perhaps some of the examples above illustrate how a Network Packet Broker can solve issues in your network or prompted some thinking about how you can increase efficiency in your environment.