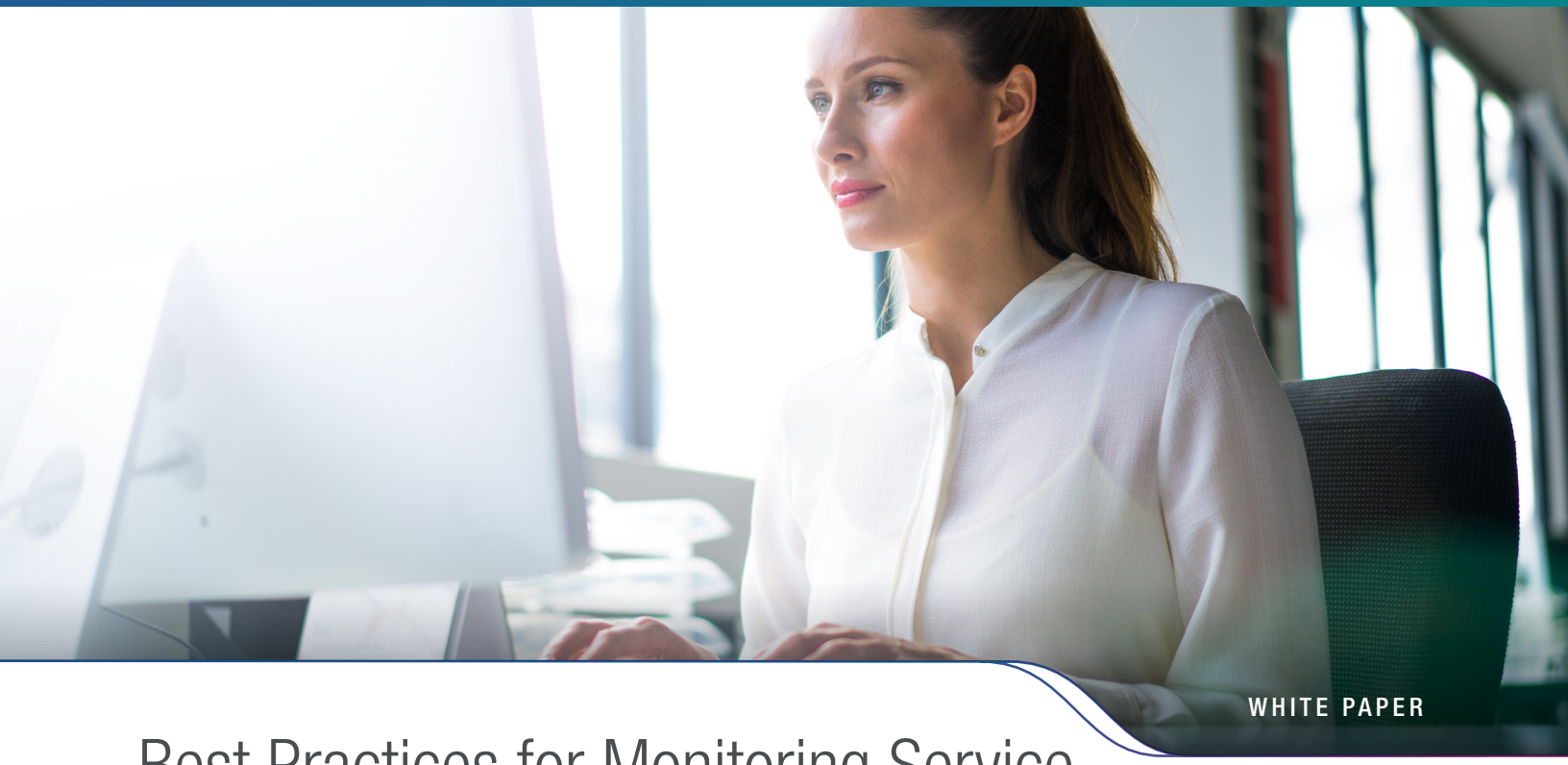

WHITE PAPER

Best Practices for Monitoring Service Provider Networks Using SPAN Ports

A network packet broker can be used to aggregate out-of-band monitoring data, filter the data as needed, and then distribute that data to the proper security and monitoring tools.

Monitoring Challenges for Service Providers

One of the challenges for service providers is to control costs while maintaining a high level of quality within their networks. Some techniques include over-provisioning SPAN port connections for IP-based traffic. This allows the service provider to make sure that there is minimal to no degradation of the packet-based traffic from those SPAN ports.

At the same time, the extensive use of SPAN and tap ports to capture the appropriate data creates other problems for service providers in regards to getting the proper monitoring data to security and monitoring tools. Mainly because monitoring tools only have a limited number of input ports but the data the tool needs may come from multiple locations spread across the network. This is where technology, like a network packet broker (NPBs) can be used to aggregate out-of-band monitoring data, filter the data as needed, and then distribute that data to the proper security and monitoring tools so that engineers can maintain the network.

A visibility architecture with network packet brokers can be used effectively to:

- Aggregate data from multiple sources (SPAN ports, taps, virtual machines)
- Lower the cost of data aggregation

KEYSIGHT TECHNOLOGIES

- Optimize security and monitoring tool performance
- Improve security and compliance initiatives

The NPB sits between network SPANs/taps and the monitoring tools where it can capture data packets and manipulate them as needed.

Service Provider Architecture Overview

The service provider network, whether it is a wireline or mobile network, needs to have a way to collect monitoring data and then filter the data as necessary. Common examples of activities that can be performed on monitoring data include: data aggregation, data distribution, packet filtering, deduplication, header stripping, packet slicing, load balancing, and specialized monitoring functions (troubleshooting, suspicious data analysis, specific data storage, QoE investigation/validation, etc.).

The following diagram shows an example of network monitoring that includes both data aggregation and data filtering/manipulation for optimum network visibility:

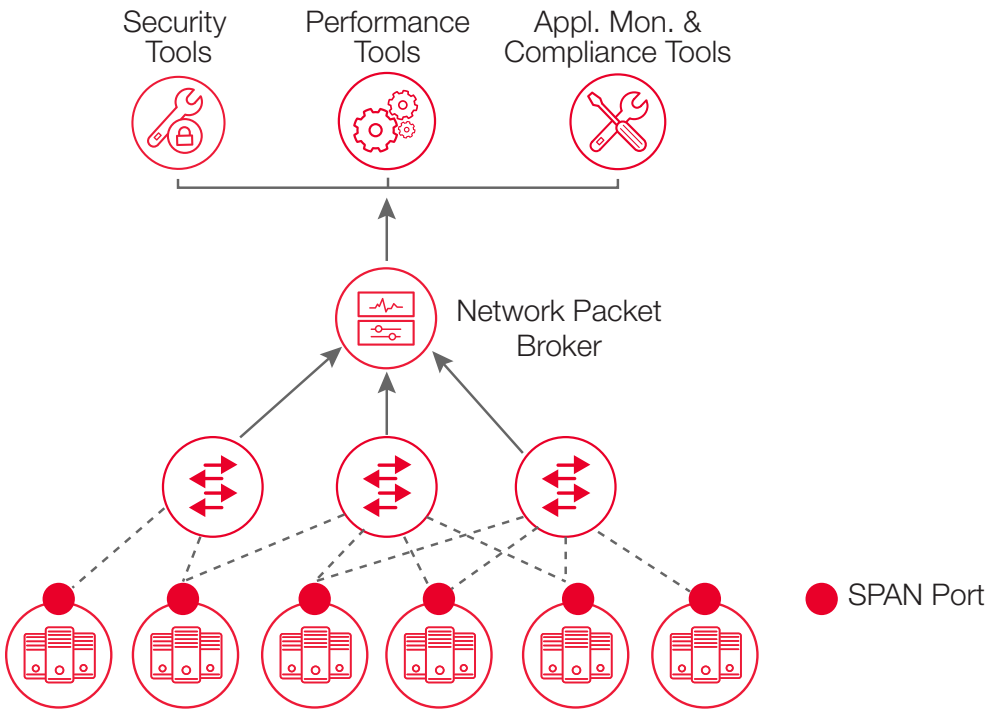

Figure 1. General Visibility for Service Providers

The exact type of data monitoring functionality needed depends upon many factors including: whether the monitoring functions take place at the edge or in the core of the network, the type of service provider network (wireline or mobile), and any particular objectives or needs that the service provider has.

Mirror ports (also known as SPAN ports) on network equipment and network taps create data access points that provide network data to the NPB. While network access points could be connected directly to the tools, the number of data access ports on security

and monitoring tools is limited. In addition, the data needs to be streamlined so that only the key monitoring data is sent to the security and monitoring tools. The NPB sits between network SPANs/taps and the monitoring tools where it can filter and forward data packets as needed.

Optimizing the Monitoring Architecture With an NPB

Service providers make huge investments in network infrastructure, monitoring tools, and policy management systems. As a result, it is essential that service providers get the most out of their investments.

Network packet brokers are a key piece of functionality to help service providers optimize their visibility architecture and maximize the return on their investment. The following list shows the most common NPB features used by service providers:

NPB FEATURES

- Data filtering
- Aggregation
- Regeneration
- Deduplication
- Load balancing
- Filter libraries
- Header stripping
- Packet trimming
- Media speed conversion
- Automation
- NetFlow generation

The following sections detail the specific features.

Data filtering

Once the data is captured and fed to the NPB, filtering can be used to remove non-relevant monitoring data. These filters can be created based upon various criteria like IP address, VLAN, port number, or application signature.

When considering an NPB, it is important to understand its filtering capabilities. Filtering is usually performed in three stages. The first stage is performed at the port where the network data enters the NPB. This is called the network port. Filtering at this location permanently removes the data for all operations downline. Once this traffic is removed, it is no longer available for analysis. So filtering at this location should be used judiciously.

The second stage of filtering is performed by a highly capable, port-independent filter that is located between the network port and the ports to which the monitoring tools, or backhaul connections, are attached. The port-independent filter, also called a dynamic filter engine, is the ideal place to perform the bulk of the filtering, as it is possible to

Once the data is captured and fed to the NPB, filtering can be used to remove non-relevant monitoring data. These filters can be created based on various criteria like IP address, VLAN, port number, or application signature.

understand exactly what is happening by looking at this location. Multiple filters can be created to effectively transfer the same data to multiple tools without clipping the data, assuming the filters are created correctly. This is what makes this location the perfect point to conduct the majority of data filtering.

The third stage of filtering is performed at the exit point of the NPB, which is called a tool port. This location does an effective job of removing unnecessary traffic on a per tool basis. However, filtering at this location can cause two problems. First, the tool port can be overrun by the volume of traffic coming from the network ports. Second, the interaction between the network filters and the tool filter is complex and not obvious unless you are well versed in set theory.

Aggregation

Network packet brokers allow the aggregation of multiple ingress links to one egress port. This allows IT to connect multiple network segments to an NPB and then send the relevant data out as a single stream to security and monitoring tools.

A benefit of removing duplicate packets is that the bandwidth of the network can be conserved, allowing service providers to postpone costly network upgrades.

Regeneration

Regeneration is the feature that allows the NPB to take data that is coming in and make a copy of that specific data so that it can be sent to multiple outputs, i.e. tools. One use case is that the same data may be needed by multiple tools (like a troubleshooting tool and an NPM tool). Another use case would be to send the data to a local tool for analysis but also send a copy to a designated SAN for additional reviews at a later time.

Packet de-duplication

Duplicate packets are most commonly caused by the use of SPAN/mirror ports. While some monitoring tools are capable of removing duplicate packets, others do not have this capability. However, even if a monitoring tool has the ability to remove duplicate packets, doing so is an extremely resource intensive task. Off-loading duplicate packet removal to the NPB can cut the CPU load of a monitoring tool in half.

Another key benefit of removing duplicate packets is that the bandwidth of the network can be conserved. This reduces the cost of data backhaul, allowing service providers to postpone costly network upgrades.

Load balancing

As the volume of data grows within a service provider's network, IT teams often find that the network data flow is increasing faster than the capabilities of their monitoring tools. A single monitoring tool that previously performed well may now be out of capacity. Through load balancing, some NPBs have the ability to send data across

multiple, similar tools and do it in a way that consistently sends all the data from a particular session to the same monitoring tool. The load balancing feature keeps session data together for better analysis, yet balances the total network load across multiple monitoring tools. This function is used extensively with network data recorders. Since session data is kept together, only one data recorder needs to be accessed to analyze any given session at a later time.

A second use case utilizes the load balancing feature to send data across multiple, redundant links within the network. Should one path fail, the NPB can send all data across one link, instead of splitting the data across two links, as during normal operations.

Filter libraries

Another time-saving feature of an NPB is the import and export of configuration information with granular control over what gets saved or loaded. Libraries of filter definitions can also be saved, allowing IT teams to create common filter definitions and disseminate these libraries for use among the teams.

Header stripping (e.g. MPLS stripping)

Removing MPLS labels increases the capability of many monitoring tools. This is because most monitoring tools are not capable of understanding MPLS-tagged packets, which means that they are unable to monitor MPLS networks. An NPB is used to remove the MPLS headers and forward the original packet contained within the MPLS tagged packet. Standard network monitoring tools can then be used to monitor activities with the MPLS network.

Packet trimming/slicing

Packet trimming removes payload data from the packet, leaving the header information, prior to sending the packet to monitoring tools. Some monitoring tools do not require packet payload information, in which case, removing payload data allows more data to be sent across the link from the NPB to the monitoring tool. As a result, the monitoring tool can receive a far greater amount of network data. Additionally, for compliance reasons, it may be desirable to “trim” or remove sensitive payload data from packets before they are sent to a monitoring tool.

If the data is being backhauled, removing the payload also significantly decreases the size of the bandwidth required for the data.

Media speed conversion

With network backbone speeds increasing to 40 and 100 Gbps, it is increasingly common that some network equipment cannot handle this higher data rate. Upgrading a network is expensive, and becomes even more costly when network monitoring tools must be upgraded at the same time. Traditionally, network engineers did not have a choice. When they upgraded their network, they also had to upgrade monitoring tools. With the advent of the NPB, network engineers now have a choice. The NPB can be used to "downshift" the speed of network data to match the speed of the available monitoring tool. Network engineers now have the ability to monitor higher-speed backbone networks with their lower-speed tools, protecting their original monitoring tool investment.

Monitoring tools, network management systems, and IT automation systems can dynamically change a NPB. Using a RESTful interface, software-based systems can control various aspects of the NPB.

Automation

Automation is a productivity enhancing option available with some NPBs. Monitoring tools, network management systems, and IT automation systems can now dynamically issue instructions to an NPB using a RESTful interface. This allows IT teams to create extremely powerful systems using multiple network devices that work cooperatively and automatically.

Another use case involves an intrusion detection system (IDS) system that detects an intrusion as it occurs. Using the automation capabilities of the NPB, the IDS sends a command that sets up a connection between the network port being monitored by the IDS and a network data recorder, immediately capturing the intrusion event for later analysis.

VLAN tagging

An NPB can be used to both generate and remove VLAN headers. In the case of adding the header, this can be especially useful for identifying where a packet came from, even after it has been aggregated with other traffic. This aids in troubleshooting and forensic analysis as the NPB can filter data based on a VLAN tag. The feature is also useful if you are using SPAN ports, as VLAN tags are not normally passed through a SPAN port.

On the other hand, certain monitoring tools do not understand VLAN headers, so an NPB can be used to remove them in those situations.

Netflow generation

Certain NPBs can generate NetFlow data and send that data to collectors on the network. This flow data can be used for multiple purposes including: network segment bandwidth overload identification, application bandwidth overload identification, application identification and filtering, problem geolocation, and performance trending. Once this NetFlow data is created, it can be sent to a dashboard or to special purpose tools that analyze NetFlow data.

Summary

Service providers are under ever-increasing pressure to modernize their capabilities to be competitive in the 21st century. This means reducing costs, improving network performance, maintaining a high level of security, and being agile enough to offer new services to customers. The right visibility solution is a key ingredient as to how well the service provider can execute on their plans.

The NPB is a necessary tool and solves many of the data monitoring issues that service providers encounter within their network including the need for:

- Cost effective data aggregation from multiple remote data points
- Removal of unnecessary data and data size reduction before transmission across the network
- Improving overall monitoring tool performance
- Providing segmented data access for special purpose tools

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