Best Practices and Use Cases for Network Visibility

WHITE PAPER

WHAT IS NETWORK VISIBILITY?

Visibility is defined by Webster's Dictionary as the "capability of being readily noticed" or "the degree of clearness." By network or application visibility, we mean removing blind spots that are hiding the ability to readily see (or quantify) what is happening on the network and/or the applications running over the network. This visibility enables information technology (IT) teams to quickly isolate security threats and resolve performance issues, ultimately ensuring the best possible end-user experience.

Another way to think about this is that visibility is what allows IT teams to control and optimize the network along with applications and IT services. This is why network, application, and security visibility are absolutely vital for any IT organization to accomplish its job. Without visibility, IT can only operate reactively to problems and will never be truly effective at eliminating those problems.

The easiest way to accomplish network visibility is to implement a visibility architecture—which is an end-to-end infrastructure that enables physical and virtual network, application, and security visibility. Once the architecture is in place, you can implement various different solutions, i.e. use cases, that you need. This white paper (and the book *The Definitive Guide to Visibility Use Cases*) will give you examples of how to leverage a visibility architecture.

The easiest way to accomplish network visibility is to implement a visibility architecture—which is an end-to-end infrastructure that enables physical and virtual network, application, and security visibility.

ixia
A Keysight Business

LAYING THE FOUNDATION FOR NETWORK VISIBILITY

Once a visibility architecture is in place, a plethora of use cases become available. As shown below, the visibility architecture introduces three fundamental layers to visibility: access layer, control layer, and monitoring layer.

Almost 70 different use cases have been defined for visibility, with many more possible, depending upon business needs.

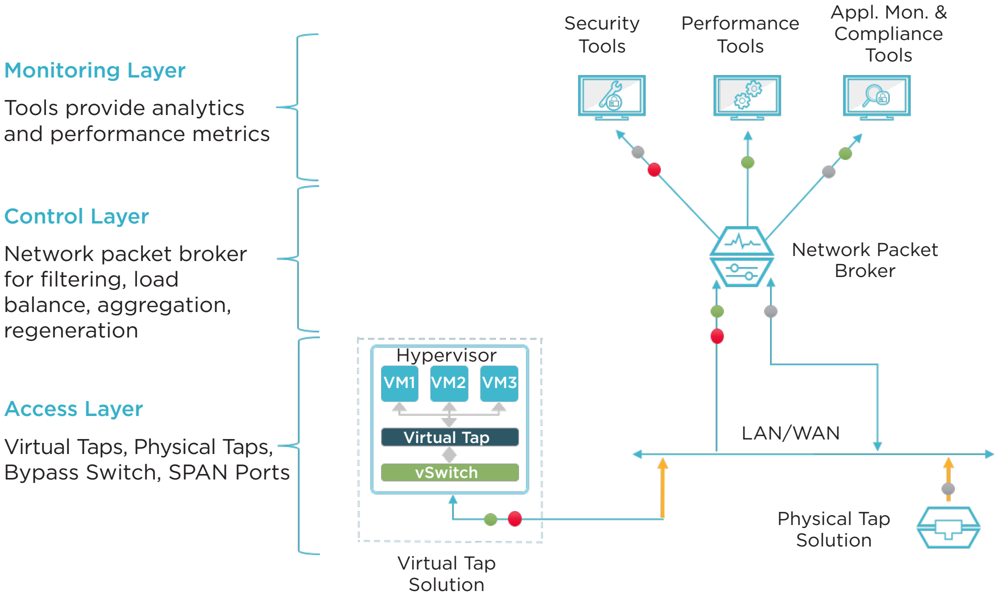

Monitoring Layer
Tools provide analytics and performance metrics
Control Layer
Network packet broker for filtering, load balance, aggregation, regeneration
Access Layer
Virtual Taps, Physical Taps, Bypass Switch, SPAN Ports
Security Tools
Performance Tools
Appl. Mon. & Compliance Tools
Network Packet Broker
Hypervisor
VM1
VM2
VM3
Virtual Tap
vSwitch
LAN/WAN
Physical Tap Solution
Virtual Tap Solution

Figure 1 - Illustration of Visibility Architecture

By using the elements shown, IT teams can solve various network and application problems. There are two fundamental categories of use cases:

- Essential visibility solutions
- Complete network visibility

Essential visibility solutions focus on network security, cost savings, and troubleshooting. These are three common pain points that affect IT on a monthly, if not daily, basis. Complete network visibility is intended to deliver more in-depth insight into the areas of blind spots, performance, and regulatory compliance.

The applicable use cases depend on the company business model (e.g., enterprise, service provider, industry), the network architecture (e.g., physical components, virtualized data center, cloud networks), and business operations (e.g., international operations, e-commerce, regulatory compliance). Almost 70 different use cases have been defined for visibility, with many more possible, depending upon business needs.

WHAT CAN YOU REALLY DO WITH NETWORK VISIBILITY?

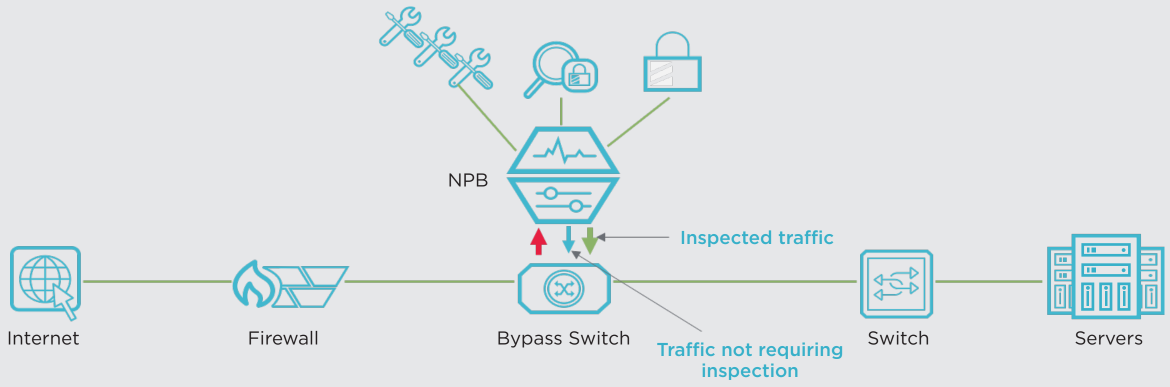
There are six distinct ways that network visibility use cases can provide clear and distinct value. They are:

- Improving network security
- Providing cost containment and cost-reduction capabilities
- Speeding up troubleshooting efforts and improving network reliability
- Removing network blind spots
- Optimizing network and application performance
- Strengthening regulatory compliance initiatives

Each one of these areas contains multiple, separate use cases. Let us look at some specific examples.

EXAMPLE #1 - NETWORK SECURITY INLINE DATA FILTERING IMPROVES SECURITY TOOL EFFICIENCY

The intent of this use case is to use a network packet broker (NPB) to create a data filter that allows low-risk data (e.g., video and voice) to bypass inspection by security tools (e.g., intrusion prevention system (IPS), data loss prevention (DLP), or web application firewall (WAF)). This uninteresting traffic can be identified and passed right back to the bypass switch and continue downstream. The advantage of this solution is that a WAF or IPS does not have to spend any central processing unit (CPU) resources analyzing irrelevant data. If your network traffic comprises a significant amount of this type of data, then you can implement this feature and reduce the load on your security tools.



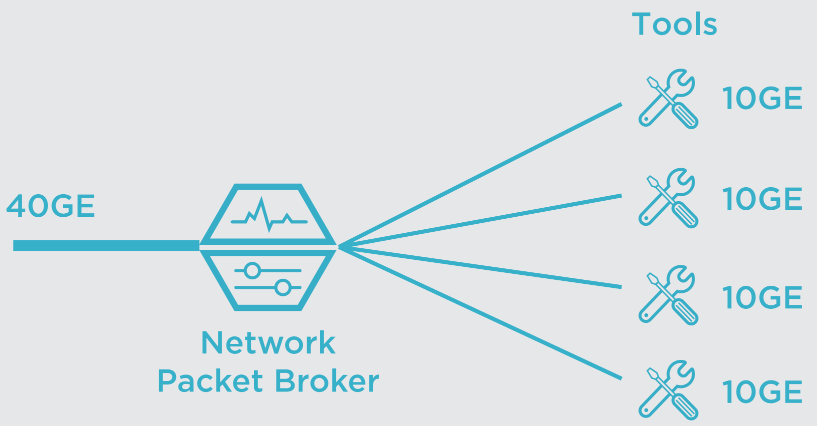
Companies deploying this use case have seen instances where up to 35% of low-risk network traffic can skip IPS inspection. This automatically increases the effective bandwidth of the IPS tool by 35% and means you may be able to delay the purchase of additional IPSs. We all know that network traffic is increasing, so you are going to need more capacity on your IPS at some point. It is really a question of whether you want to minimize the costs you will incur, or not.

Companies deploying this use case [inline data filtering] have seen instances where up to 35% of low-risk network traffic can skip IPS inspection. This automatically increases the effective bandwidth of the IPS tool by 35%.

EXAMPLE #2 - COST CONTAINMENT LOAD BALANCING EXTENDS THE LIFE OF 1–10 GBPS TOOLS IN 40 GBPS NETWORKS

A second example use case involves decreasing network equipment costs. This is accomplished by using the NPB to load balance data to security and monitoring tools. There are a couple of clear examples of how load balancing can help most enterprises. First, network traffic increases, along with traffic speed increases, are very common occurrences. But what about the monitoring impacts of the bandwidth upgrades? For instance, if you upgrade your network core from 1 Gbps to 10 Gbps, you will now need 10 Gbps tools to properly monitor it. If you upgrade to 40 Gbps or 100 Gbps, there may be few to no monitoring tools available at those data rates. And, available tools at those data rates can be very expensive.

Packet brokers provide the aggregation and load balancing capabilities needed. Data coming into the packet broker can be broken down into lower-rate streams of data and then sent to the proper monitoring tools. For instance, load balancing of 40 Gbps data allows you to spread the monitoring traffic across multiple 10 Gbps tools. This obviously assumes you have enough 10 Gbps tools for the load. Once you implement this, you can extend the life of your 10 Gbps tools a little longer until you have enough budget to purchase more expensive tools that can handle the higher data rates. For instance, you might implement the network upgrade you want to this year and then purchase additional higher-rate monitoring tools later.



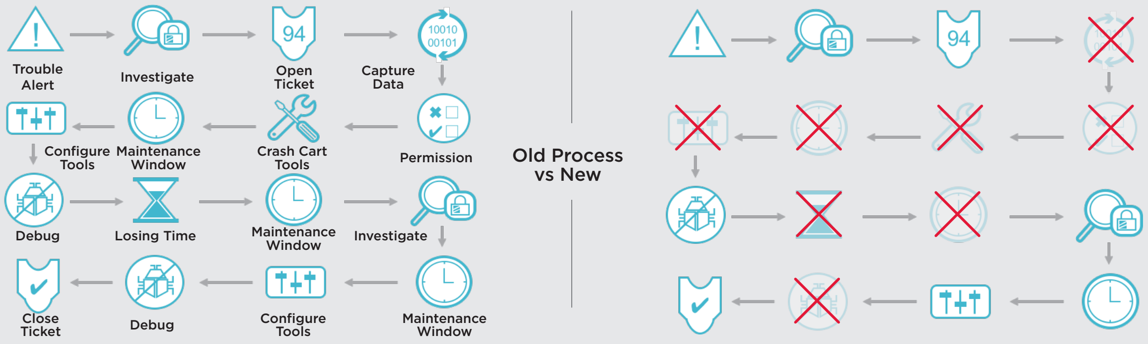
Another example is to pool your tools in one location and feed them the data they need from a packet broker. Some architectures use individual tools spread out across the network. This may have some minor access advantages, but these tools are often underutilized. 2016 survey data from Enterprise Management Associates (EMA) show that 32% of enterprise tools are under loaded, i.e. less than 50% utilization. Tool centralization and load balancing allows you to pool your resources and increase utilization by using fewer devices. You can often postpone purchases of additional tools until the utilization factor is high enough to warrant additional ones. This obviously assumes you have enough 10 Gbps tools for the load. Once you implement this, you can extend the life of your 10 Gbps tools a little longer until you have enough budget to purchase more expensive tools that can handle the higher data rates. For instance, you might implement the network upgrade you want to this year and then purchase additional higher-rate monitoring tools later.

2016 survey data from Enterprise Management Associates (EMA) show that 32% of enterprise tools are under loaded, i.e. less than 50% utilization. Tool centralization and load balancing allows you to pool your resources and increase utilization by using fewer devices.

EXAMPLE #3 - TROUBLESHOOTING TO REDUCE/ELIMINATE THE NEED FOR CHANGE BOARD APPROVALS AND CRASH CARTS

Once visibility equipment (like taps and NPBs) are installed into the network, you rarely have to touch the network again. This allows you to optimize several of your troubleshooting processes to gain new efficiencies.

For instance, once a tap is installed, it is “set-and-forget” technology and will sit there passively forwarding a copy of all traffic to the NPB. Since the monitoring data is copied by the tap, you can do whatever you want, because it will not affect the network. This has the huge benefit of eliminating most, if not all, Change Board approvals for troubleshooting purposes. You have already got the data access. If you combine that with a packet broker, you have instant access to pretty much all the data you need across your whole network for troubleshooting. There is no need to wait 2 hours, 2 days, or 2 weeks for permission to touch the network.



This process reduction is shown in the image above. The left side shows a typical, basic process overview. An alert happens and you investigate it, open a ticket, ask for Change Board permission to touch the network, assemble the crash cart, wait for a maintenance window, then you finally get some troubleshooting time in, but you do not have enough time, so you do it all over, finally resolve the issue, and then close the ticket. On the right hand side, you can see where the effort is literally cut in half.

Unless you are touching some mission critical component, you can skip Change Board approval and go straight to debugging—no crash cart or maintenance window needed. Authentication, authorization, and accounting (AAA) rules are typically preserved by the packet broker, as well, which further reduces the need for Change Board approvals. This new process has a big impact on reducing the mean time to repair (MTTR). Case studies show that customers can reduce their MTTR by up to 80%.

CONCLUSION

Network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. There are many use cases that can be deployed to solve or enhance issues that IT monitoring and security engineers face. The key point is to implement a visibility architecture that creates the fundamental capture and sharing of the valuable data needed.

> This new process [reducing the number of Change Board approvals and the use of crash carts] has a big impact on reducing the mean time to repair (MTTR). Case studies show that customers that can reduce their MTTR by up to 80%.

Use cases based on a visibility architecture will allow you to do the following:

- Access the data you need, when you need it, across the network to properly diagnose problems
- Add/remove security, forensic, and monitoring tools at will for inline and out-of-band monitoring architectures
- Decrease MTTR
- Provide a rapid response to crises
- Conduct advanced threat analysis
- Eliminate most, if not all, Change Board approval processes and crash carts for monitoring efforts
- Reduce the cost of a breach by connecting tools to the network faster and decreasing the associated MTTR
- Reduce your tool (and SPAN) port programming effort and costs

An extended list of almost 70 visibility use cases can be found in the full-length book, *The Definitive Guide to Visibility Use Cases*. For more information on network monitoring solutions, visit www.ixiacom.com/solutions/network-visibilty.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127