Network Visibility for the Digitized Enterprise

Authored by
David M. Davis &
Scott D. Lowe,
Partners, ActualTech Media

Your Guide to Seeing It All with a Comprehensive Visibility Solution

ActualTech Media
DATA CENTER INNOVATIONS
LEARNING SERIES

DATA CENTER INNOVATIONS LEARNING SERIES

Network Visibility for the Digitized Enterprise

Authored by
David M. Davis & Scott D. Lowe
Partners, ActualTech Media

ActualTech Media

Data Center Innovations Learning Series
Network Visibility for the Digitized Enterprise

Author:	David M. Davis & Scott D. Lowe, ActualTech Media
Editors:	Hilary Kirchner, Dream Write Creative, Rachel Burdick, WordNerd Services
Book Design:	Braeden Black, Avalon Media Productions Geordie Carswell, ActualTech Media
Layout:	Braeden Black, Avalon Media Productions

Printed in the United States of America

First Printing, 2016

ISBN 978-1-943952-15-1

ActualTech Media
Okatie Village Ste 103-157
Bluffton, SC 29909
www.actualtechmedia.com

Table of Contents

About the Authors

David M. Davis,
Partner, ActualTech Media

David Davis is a partner and co-founder of ActualTech Media. With over 20 years in enterprise technology, he has served as an IT Manager and has authored hundreds of papers, ebooks, and video training courses. He's a 6 x vExpert, VCP, VCAP, & CCIE# 9369. You'll find his vSphere video training at *www.Pluralsight.com* and he blogs at *www. VirtualizationSoftware.com* and *www.ActualTech.io.*

Scott D. Lowe,
Partner, ActualTech Media

Scott Lowe is a vExpert and partner and Co-Founder of ActualTech Media. Scott has been in the IT field for over twenty years and spent ten of those years in filling the CIO role for various organizations. Scott has written thousands of articles and blog postings and regularly contributes to *www.EnterpriseStorageGuide.com* & www.*ActualTech.io.*

About ActualTech Media

ActualTech Media provides enterprise IT decision makers with the information they need to make informed, strategic decisions as they modernize and optimize their IT operations.

Leading 3rd party IT industry influencers Scott D. Lowe, David M. Davis, James Green and special technical partners cover topics of interest to IT pros and that are driving change in the modern enterprise.

Cutting through the hype, noise and claims around new data center technologies isn't easy, but ActualTech Media helps find the signal in the noise. Analysis, authorship and events produced by ActualTech Media provide an essential piece of the technology evaluation puzzle.

More information available at **www.actualtechmedia.com**

ActualTech Media

Book Features

In Depth

Takes readers into the deep, dark depths of a particular topic.

In The Book

Points readers to a related section of the book where they'll find more information.

1

What Is Visibility?

Have you ever dreamed of seeing the world from space? Imagine flying high above the clouds as the Earth spins beneath you. For people like you and me to be able to make a dream like this a reality, NASA has made available a viewer that connects to a high definition camera mounted to the International Space Station, from which you can see the Earth from space in *real time*. Aside from allowing you to avoid the difficulties of personally attempting to achieve Earth orbit, this tool helps you to quickly appreciate what it's like to see everything from that view. You may also quickly realize that while you're seeing *everything*, you are, at the same time, seeing *nothing*. With such a wide and high perspective, all of the data—the people, the roads, the buildings, the states, the remaining dinosaurs—may be there, but it is difficult to make out what any of it means. This situation is similar to one that exists in the world of IT network visibility.

Beneath every organization's firewalls, intrusion prevention systems, compliance tools, big data analytics tools, buzzword-of-the-year tools, etc., lie the pulsing tentacles of the visibility infrastructure, feeding data to all of those components. Visibility enables you to see your data wherever it goes—at a high level or low level. For example, high-level visibility might allow you to stalk your data as it moves across multiple cloud providers, or as it meanders across your organization's multiple branch locations and datacenters worldwide. Visibility into low-level areas, on the other hand, can allow you the granularity to isolate one specific application packet flow coming from one specific network device.

Visibility Defined

Visibility is the term used to describe a data distribution layer that intelligently connects raw, unprocessed incoming data to your analytics and security tools. It is not some sort of data analytics or monitoring application, or even deep packet inspection. Visibility is pure and simple data distribution with the ability to intelligently direct and load-balance data flows to optimize security and network performance.

True visibility facilitates both high-level and low-level insights.

Just like you assume—or hope—the water you are drinking from your tap at home doesn't contain brain-eating amoeba, most technology people assume—or hope—that the data being fed into their analysis and security tools is complete and untainted. In reality, thanks to the rise of hybrid and public cloud, the modern organization's network edge has been fading for years, making the situation a bit murky. The drive to cloud services combined with exponential increases in traffic and a wide range of Internet of Things (IoT) automation have contributed to some blind spots and other areas with limited visibility.

Unfortunately, many IT organizations think more about the capabilities of their security and monitoring tools than they do the visibility infrastructure that feeds data to these tools. There are a couple of possible reasons for this:

- They believe that they already have all the visibility they need (and don't go looking for more)

- They do not know how best to evaluate a visibility solution

The end result is blind spots that limit visibility into enterprise applications and data flows. The organizations themselves and their end-users both suffer the penalties:

- Application performance problems

- Downtime

- Worst of all: data breaches

How Far Does "Visibility" Reach?

Today's modern enterprise is a complex organism, constantly evolving further away from its strict legacy data center roots. More and more, enterprises are moving to a hybrid cloud model where they use elements of both private and public clouds.

The hardware side of the hybrid cloud is made up of traditional servers, storage, and network infrastructure; stuff you've come to know and... (insert relevant emotion here). On the software side, faster deployment demands are driving the industry to virtual implementations and software as a service (SaaS) applications. Each element mentioned above might be supported by a different operating system, database, and security solution. Each piece of hardware and software that makes up your particular enterprise cloud is an 'opaque container' into which you may or may not have visibility.

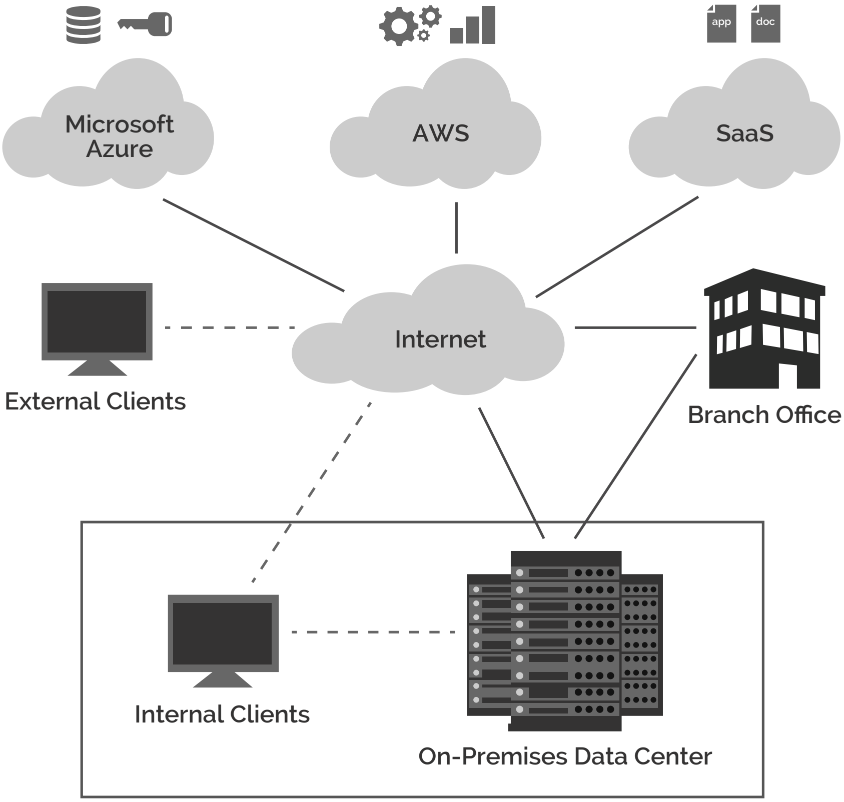


Figure 1-1: Sample hybrid cloud configuration spanning on-premises, branch office, public IaaS, DBaaS, and SaaS. Each its own opaque container.

Visibility requires the ability to peer into any of these opaque containers so you can monitor how many of your resources are in use, who is using them, where bottlenecks might exist, whether your infrastructure is secure, and much more.

Anyone responsible for today's complex infrastructures needs to have visibility into all of their traffic without regard for their deployment configuration or where their data resides.

Why Is Visibility So Challenging to Obtain?

According to a 2016 survey conducted by Rightscale, modern enterprises are employing at *least six clouds,* on average. While a single cloud network may cause visibility issues, six or more networks will most certainly create visibility blind spots as IT struggles to access data from these myriad networks—some of which they don't even own. Making matters worse, IT organizations are now caught in a constant cycle of deploying new services, supporting new use cases, managing growth, and trying to "see it all" at all times.

Figure 1-2: As applications and data are distributed more and more across multiple clouds, the visibility challenge is exacerbated

Is There Such a Thing as Too Much Visibility?

Unless you're a used furniture store that goes out of business every 9 to 12 months, your organization has to live within its means. You also need to make sure you protect your stakeholders. Visibility is all about having sufficient access and capacity to support your business today, tomorrow, and for the next three-to-five years. Ask yourself these questions:

1. Do I expect my traffic to grow in the next 36 months?
2. In that same timeframe, do I expect to integrate additional cloud applications, cloud-based security, and cloud-based monitoring?

Creating the right size network visibility solution allows your organization's business to grow without having to 'rip and replace' your infrastructure as you add more traffic and more applications to the mix.

Levels of Network Visibility

If you were constructing a 3-story building, you would need a foundation designed to support a 3-story building. Would you use that same foundation if you suddenly got approval to increase your building to 10 stories? How about 20 stories? Probably not. If you do, let me know where it is so I can stay away!

Figure 1-3: How many stories can you add to this building before the foundation is insufficient to support it?

You want to select a visibility and data distribution architectural foundation that is the right size for your business today, but also allows for growth in the future.

Thus, true *network visibility* means:

- The ability to access all of your data from any location without dropping packets or adding latency to your business

- Intelligently distributing it to your security and analysis tools

That's not too much to ask, is it?

5 Reasons You Need Network Visibility

We covered what network visibility is and how it adds value, but why is it that companies of all sizes need network visibility?

(Yes, even yours.)

Here are the top five reasons:

1. **Troubleshooting application performance issues**
   In many cases, application performance is tied to network performance, much to the chagrin, dismay—and sometimes, outright protestations—of network administrators around the globe. When applications "run slowly" or stop working, you need real-time network diagnosis and problem remediation so you can solve network issues quickly and get applications running again. You need to be able to quickly identify the *root cause*, and not just chase after symptoms. A proper visibility solution will allow you to immediately isolate the application, the user, and the device so you can look for and resolve bottlenecks.

2. **Monitoring application performance and reliability**
   You need applications to perform not just today, but for the long term. Network-centric applications need to be continuously and precisely monitored for reliability and performance. You've heard the phrase "Garbage in, garbage out." In that same vein, application monitoring tools are only as effective as the data stream they are fed.

3. **Ensuring network scalability**
   Over time, your network and traffic volume will change, and, if history is a reliable forecaster, it will probably grow really quickly. The data that many applications send across networks

is "bursty." In this context, *burstiness* refers to sudden spikes over short periods of time before traffic levels return to normal. We hate to *burst* your bubble, but this means that you must account for the average network utilization **and** for the peak network utilization created by bursts of traffic.

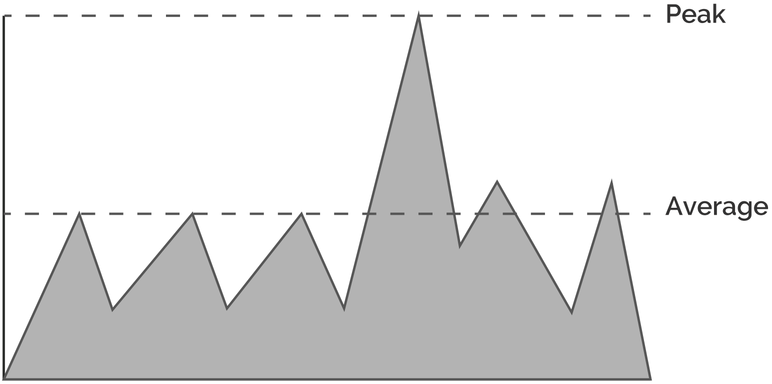


Figure 1-4: A visibility solution must be able to support peak network utilization, not just average traffic

To provide that network scalability, you'll need visibility during the peak spikes as well as during periods of growth in your average traffic volume. As is true for highways and buildings, once your visibility architecture hits its maximum capacity, upgrading becomes more expensive. It's really tough to add lanes to existing highways and it's tough to add more floors to a highrise. You will save money in the long run by having growth capacity in your visibility architecture.

4. **Protecting and securing the network**
   Instances of malware and distributed denial of service (DDoS) attacks have grown exponentially every year since they were first observed. Every time there is a new attack, there is a firewall upgrade, intrusion prevention device deployment, or other network security feature that needs to be integrated to counter

it. Protection has become a verb in the network security world, necessitating constant changes and updates. The more security tools you integrate, the more resilient a visibility foundation you need to host them on.

5. **Managing complex network infrastructures**
   Today's networks have grown more and more complex with the addition of multiple data centers, data encryption, additional security and analytics tools, and of course worldwide mobile users demanding instant access all the time. No pressure, right? The monitoring tools you use will ensure excellent performance, but *only* if you are seeing all of the data in a timely manner.

Picking the Right Size

Different networks have different levels of complexity, different applications, different availability requirements, and different security requirements.

When considering what level of visibility you need, here are some questions you need to ask yourself.

- **How critical is application delivery speed?**
  Everyone says speed is important, until they start having to make tradeoffs. If you are in the financial industry, for instance, achieving latency in the milliseconds may be critical; whereas in the medical industry, they can afford full seconds. As you work to get closer to zero latency, your costs will increase exponentially, hence the tradeoffs. That said, many companies have high performance applications that require consistent low latency. Examples include audio/video streaming, virtual desktop infrastructure (VDI), and financial applications.

- **How critical is application reliability?**
  Companies can be like kids; they want *all the things* all the time. *Every* company wants continuous uptime for their applications. For some, however, achieving consistent uptime isn't an optional outcome. An always-on business, such as an overnight shipping firm, might lose millions of dollars per minute of downtime. An airline might lose tens to hundreds of millions of dollars if their network were to go down for even part of one day.

- **How secure do I need my network and data?**
  With huge breaches making the headlines every ~~year month~~ week, security is important to everyone—except, perhaps, the nefarious denizens of the hacking underworld looking to plunder your systems! Visibility across the network—regardless of the complexity of the network—is needed for security tools to adequately defend the network. Beyond security is private data protection. Certain data elements, such as personally identifiable information, or PII, require special care and protection to ensure that information is kept safe from prying eyes. Companies in healthcare, financial industries, and even retail are under regulatory mandates that require them to protect this personal information. The visibility infrastructure needs to be able to go beyond simply pushing data to compliance-monitoring tools; it also needs to mask sensitive information to ensure adherence to legal and other compliance requirements.

- **How complex is my network infrastructure?**
  Increasingly, organizations are running applications across multiple data centers and hybrid clouds. They are also often connecting IoT devices to their networks and allowing employees to use their personal mobile devices to access company networks. *What could go wrong?* With all of these activities, having visibility into the traffic flowing on and off of those networks has become critical.

Signs That You Need Greater Visibility

In many cases, it can be tough to determine if you have adequate levels of performance and security for your company's applications, but there are some tell-tale signs that you need greater visibility.

You need greater network visibility if you . . .

- Have experienced a security breach in the past 12 months
- Have experienced network outages
- Experience unexplained application sluggishness
- Have areas of your network into which you have no visibility or limited visibility
- Are implementing secure SSL communications

When you have an application problem or network outage, do you find yourself saying, *"Hmmm... I bet something's wrong,"* or are you able to pinpoint the problem area right away? If it's the former, you may be in a need of a better visibility solution.

Next Steps

If you are providing applications to end users or customers, visibility across your entire network is critical to ensure their safety and yours.

In the next chapter, we'll jump into the good, the bad, and the ugly of today's network visibility tools. Read on!

2

When Good Isn't Enough

Visibility sits at the very foundation of the network. The network relies on visibility to deliver data promptly and accurately. The visibility layer connects to—and collects data from—all kinds of sources, and makes sure every data flow gets distributed and load-balanced across security and monitoring tools. Sounds straightforward enough…

But, as with all things IT, there's just a bit more to the story.

There comes a point at which attempting to process these data streams is like trying to deliver a higher volume of water to your house without installing the new pipes necessary to handle more volume. You can turn up the water pressure coming to your house, but if the existing pipes can't handle that pressure, they'll start to leak, and will eventually burst. You can say something similar about the "pipes" in your visibility environment. For visibility environments, there is a lot of data coming from a lot of sources, and it does not come in at one constant rate. It spikes. At times, it spikes a lot, and you can't afford to lose any of that data. Don't let traffic spikes burst your visibility pipes.

Adding to the challenge, your good data—you know, the stuff that keeps your business actually *in* business—might be mixed in with malware and attack traffic that needs to be quarantined and annihilated. You also have to balance increasingly burdensome compliance requirements, which may mean masking any personal information that might be hitching a ride in your network's data packets. You need to collect, time-stamp, and store some of the data for potential future forensics just in case you need to go back and look at it. If your business applications require high availability, you might also have dual/redundant paths to eliminate single points of failure and prevent downtime. That means *every connected tool* needs to be monitored so traffic can be rerouted in case of a failure or maintenance requirement.

All of this impacts the visibility layer. It turns out your visibility layer is dealing with a lot more than you thought. *What could go wrong?*

Well... that's where things start to get really complicated.

Let's Start with Data Access

The most basic building block of a visibility architecture is data access. You would think this would be straightforward, but as you learned in Chapter 1, a lot of company services are now scattered in a variety of data centers or branches. Some of it resides in various public clouds, and some resides in your own data center.

Tapping in to each of these data sources is the first step. The simplest and most straightforward method is to configure *port mirroring.* Port mirroring is accomplished by creating a SPAN port—Switch-Port ANalyzer—to copy traffic from a source to a destination (where the source and destination could be, for example, a server and a monitoring device).

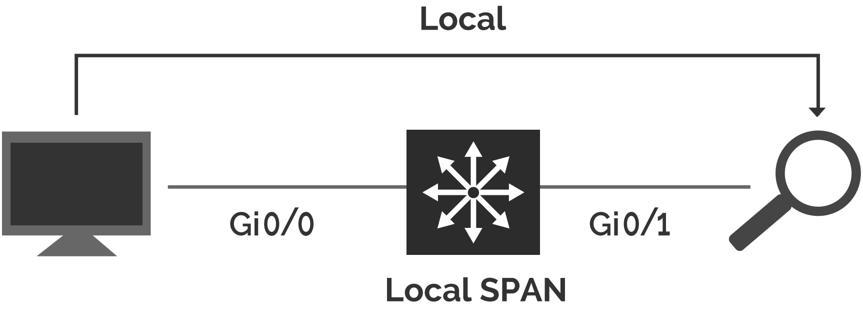


Figure 2-1: A SPAN port simply mirrors traffic from one device to a second device. Under a high load, SPAN ports can lose data

If you're in a supremely simple data center, this might be a "good enough" solution for very basic packet capture when the port mirroring switch can actually handle the traffic flow. However, in many cases, switches simply can't keep up the mirroring due to the throughput of the data, and data is lost without you even knowing it.

Remember: Your security tools are only as good as the data that they can see and identify.

Imagine your gigabit switch ports are those aforementioned water pipes. Even at single gigabit data rates, SPAN ports struggle to keep up. Just imagine the apocalyptic scenario that arises when you start to throw 10 Gb and faster links into the equation. At single gigabit speeds, even Cisco® acknowledges that when a switch is under heavy load and must choose between passing normal traffic and SPAN data, the SPAN data loses the contest, resulting in mirrored frames being arbitrarily discarded.

"Other than that, how was the play, Mrs. Lincoln?"

Network taps are typically more reliable than SPAN ports, particularly at higher data rates. Even better, they don't add additional jitter or change the timing like a SPAN port can at high data rates. Having an array of physical and virtual tap options allows you to connect to dedicated or virtual data sources.

Living in a Post-Access World

Now, imagine that you have a bunch of network taps and you have rivers of data coming to your visibility layer. The unfortunate reality is that you actually have the same data coming in multiple times because taps might have overlapping domains.

You are about to find out exactly what deduplication is all about – and why it is critical to your success.

The purpose of deduplication is to eliminate duplicate copies of data without losing any original data in the process. Although this might sound easy enough, as you might imagine by now, there's just a bit more to uncover here. For example, at gigabit per second speeds, not all deduplication algorithms get the job done. At even greater speeds, the situation becomes increasingly more grim.

When deduplication fails to work correctly, you end up with multiple copies of the same traffic mixed in with missing traffic. To say that this scenario creates a mess for your security and analysis tools is like saying that Los Angeles roadways are "a little congested."

Shaping the Data

By this point, you have all of the data, it's deduplicated, and you have taken care of any data spikes that might exist. Now, you can start considering how you want to distribute the information. The first step is to make sure you can actually read what you're getting, even when significant portions are encrypted. Although you could leave decryption to the upper layers, doing so within the visibility layer allows you to better distribute information to the proper tools.

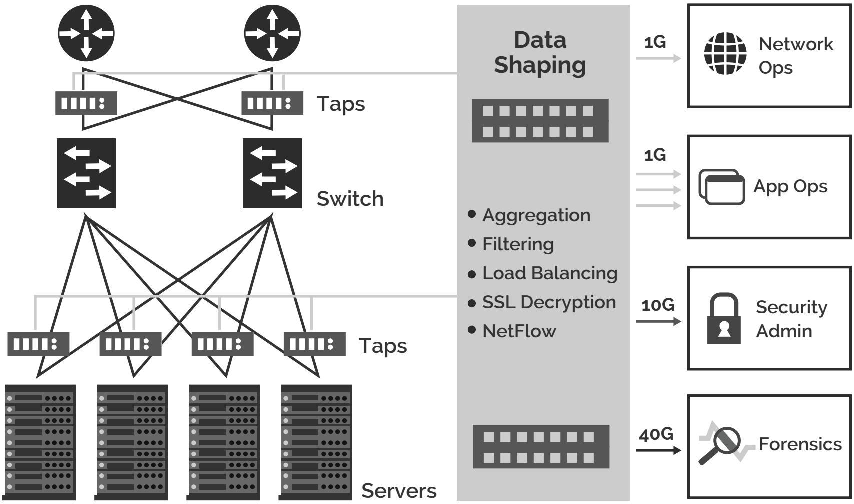


Figure 2-2: The visibility layer "shapes" the data to present only the right data to the right tools in the right state

Creating a Stable Foundation

Imagine you're buying a house. You drive up to the curb with a real estate agent in tow and see a *really* nice house, but it's sitting at a 45-degree angle because half of the foundation is rotted away. Rarely do people say, "You know... I'm ok with that! It'll be an adventure trying to walk uphill across the living room!"

One thing you can say about every foundation is that people—in this case, network and security teams—count on them to be both reliable and trustworthy. Depending on the needs of the organization, you may have a single path, dual redundant paths, or you may want to have multiple redundant paths for incoming traffic. Additional redundancy provides options for traffic flow in case any single tool experiences an unexpected outage.

High availability paths require your visibility layer to:

- Support redundant paths
- Be able to actively monitor and verify the status of every network tool
- Be able to easily and accurately program the flow paths

Not all visibility solutions provide the ability to coordinate between network packet brokers. This capability is critical if you want to support high availability redundant paths.

Network Packet Brokers

Network packet brokers are intelligent data distribution devices used to access and transform data into a format that security and network analysis tools can use. You will learn more about these devices in Chapter 3.

Let's get a bit technical for a second. Verifying network and security tool status requires a heartbeat function between the network packet broker and the tools to know when the heartbeats stop and start. With a resilient architecture, you can deploy tools in succession; for example, a firewall followed by an intrusion prevention system. But it also means you have to have failover options. When a tool fails, a hot-standby path can be used. Or, depending on the importance of the tool, you may choose to route around it instead.

Of course, programming all of these primary and secondary paths requires a lot of connections. If you are using command line interfaces (CLI) to manually program those connections, you may soon be attending a carpal tunnel syndrome sufferers' support group. Moreover, as unlikely as it seems, you might (gasp!) make a mistake! Any issue with just *one* of those commands, and you may have just created a connection to nowhere. If your typing mishap doesn't result in an error message, you may walk away pleased with yourself for a job well done when, in fact, you've just routed traffic that was meant to be analyzed directly into a black hole. A drag-and-drop GUI that automatically analyzes and deconflicts connection errors is a much more reliable programming solution.

Where Visibility Must Be Improved

Companies using older network visibility solutions that have been cobbled together over the years are about as stable as a tower of stacking blocks with a bunch of lower pieces missing. One wrong move, and your efforts are wrecked.

Figure 2-3: As network infrastructure ages and disparate solutions aren't adequately integrated, stability begins to fade.

Visibility must be improved so that IT organizations have:

- **Complete monitoring and root cause analysis** to identify and troubleshoot network issues
- **Problem prediction and prevention** to avoid issues
- **Complete visibility for security solutions** that need access to network traffic
- **Complete visibility for network analysis** from a high level to a low level, and even down to deep packet analysis

Next Steps

In the next chapter, you'll learn how to increase your visibility. You'll find out in greater detail what to look for in a visibility solution, and what makes for a successful visibility implementation.

3

Taking Visibility Up a Notch

What makes one visibility solution amazing while another just barely scrapes by? Just as with cars, it all comes down to features, and the performance of the engine.

If all you have is one or two connections going into a firewall, and you need one tap to support a single analysis tool, there are lots of solutions you can choose from. It's when you need more resilience, higher data rates, and more tool connections that the list of viable options pares down quickly.

Some vendors claim they offer comprehensive visibility, but what does that mean? When it comes to your network, you need a solution that provides total access, solid resilience options, and can handle high data rate distribution across many tools. That set of requirements forces you to take things up a notch.

What Makes a Visibility Implementation Successful?

If you are firing a missile, you definitely want it to know the difference between an enemy tank and a school bus. The consequences for confusing the two would be catastrophic. Similarly, if you are fine-tuning the quality control cameras on a farm's assembly line, you would definitely want your system to know the difference between a tomato and a rock.

When it comes to data, you want to know how to differentiate between good data sources and bad ones.

Starting at a high level, what makes a visibility solution better than average? The engine. And the engine can only perform properly if it's supported by a stable frame.

It Is Resilient

If you had to prioritize between strong and nimble, which is more important? The reality is that you need both. Most businesses expect to grow, for threats to increase, and for employees to demand more. Being prepared for those expectations to become reality demands resiliency, flexibility, expandability, and scalability in all things IT, which starts with your visibility environment.

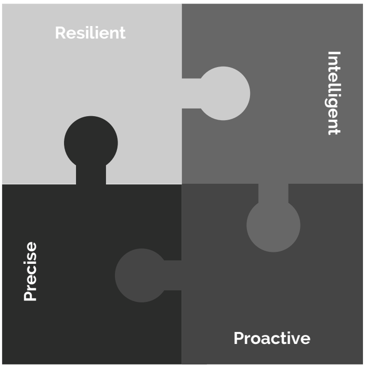


Figure 3-1: Characteristics of a strong visibility solution

Lots of organizations are still hesitant to place their security solutions inline. *That concern is so 2010*! As long as you have a good bypass switch, the ability to monitor all of your tools with a fast heartbeat, and the responsiveness to rapidly route traffic around outages, you are ready to take off the training wheels and go inline! Resiliency enables inline operations, allowing for better, faster network protection.

Let's look at the bypass switch. If you are going to go inline with your security, you absolutely need one of these. Sure, you can get a visibility solution with an *integrated* bypass switch, but, let's get serious for a second. Every piece of equipment fails sooner or later, and requires maintenance. If, for instance, your bypass and your network packet broker fail at different intervals, why would you want to take one offline during the other's maintenance? Instead, to minimize the potential of a single problem from taking out your visibility environment, you should consider a separate bypass switch and packet broker.

The next consideration is what kind of bypass switch to use. It turns out they are not all the same. Programming them can be a bit cumbersome if you don't have a nice drag-and-drop GUI. You should also have lots of heartbeat options and be able to program active-active or active-standby modes. Active-active mode allows you to load-balance between two active devices. Active-standby allows you to have a primary, and a hot backup, in case of failure. You should also be able to program the bypass switch to fail open or closed, depending on your needs.

Resilient designs also improve network security deployments by helping to improve the efficiency of inline security tools and security operations teams, ultimately freeing resources for even greater focus and investment. Basically, it's about *doing more with less* (a phrase that senior management loves to hear).

As shown in **Figure 3-2**, once in place, a resilient solution allows you to adopt a best-of-breed posture. You get to choose the best bypass switch to pair with the best network packet broker to deliver the best load-balancing and context-aware data filtering. This setup can identify applications and ensure they are routed properly. It provides security intelligence that decrypts traffic and masks personal information in your data.

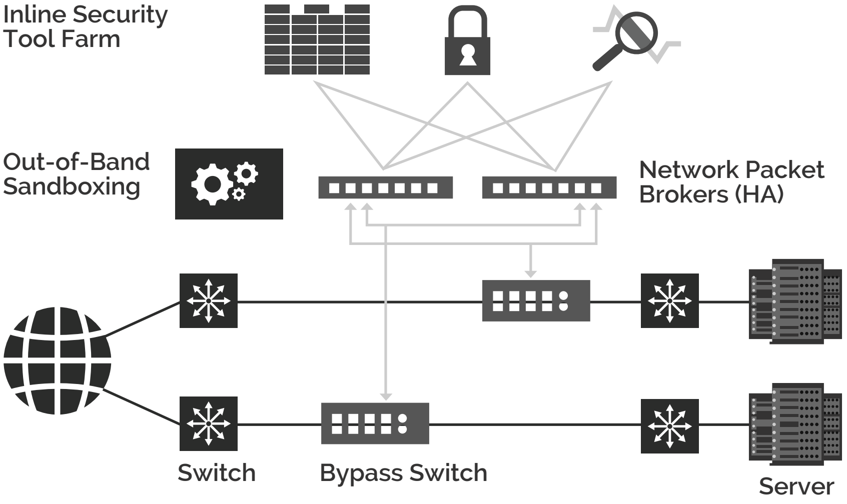


Figure 3-2: A resilient visibility solution

Resilience means you never lack choices. You want to choose where traffic should be routed, which traffic to inspect versus what you may decide you trust, and as many failover paths as you need to give you backups in case of outages.

It Is Intelligent

One person's smart is another person's... well, not so smart. How do we measure intelligence in something like a network visibility infrastructure? Is it like electricity? As long as it turns on and doesn't burn down the house, we are happy? But then what about Nest, a company that managed to turn a really, really boring market—home thermostats—cool again by introducing smart thermostats, which also manage to save users a lot of money at the same time? What if your visibility infrastructure could transform your network experience like that?

Intelligent visibility means never having to blast every tool with every piece of data because your visibility environment isn't smart enough to send your tools *only* the data they need. It means never dropping packets because your environment can't handle the pressure of high volume traffic. It means being able to decrypt traffic in real-time; precision time-stamp every packet; verify application server authenticity; and geo-locate devices. It means the ability to be smart about which data you distribute to which tool. It means not just being a basic switch.

The real goal is to give out-of-band monitoring tools a broader view of the network by providing easy access to both network traffic and external intelligence, and to conversely allow those same tools to efficiently focus on the details that matter most. It is also the goal to give in-band tools all of the data quickly and efficiently.

If you look at a configuration like **Figure 3-3**, you can see it is all possible:

- **Total access** to network traffic from any location
- **Data filtering** and grooming
- **Decryption** of SSL traffic for monitoring
- **NetFlow** generation with extended contextual metadata
- **Data masking** of sensitive content (e.g., credit card numbers)
- **Load balancing** of traffic across monitoring tools

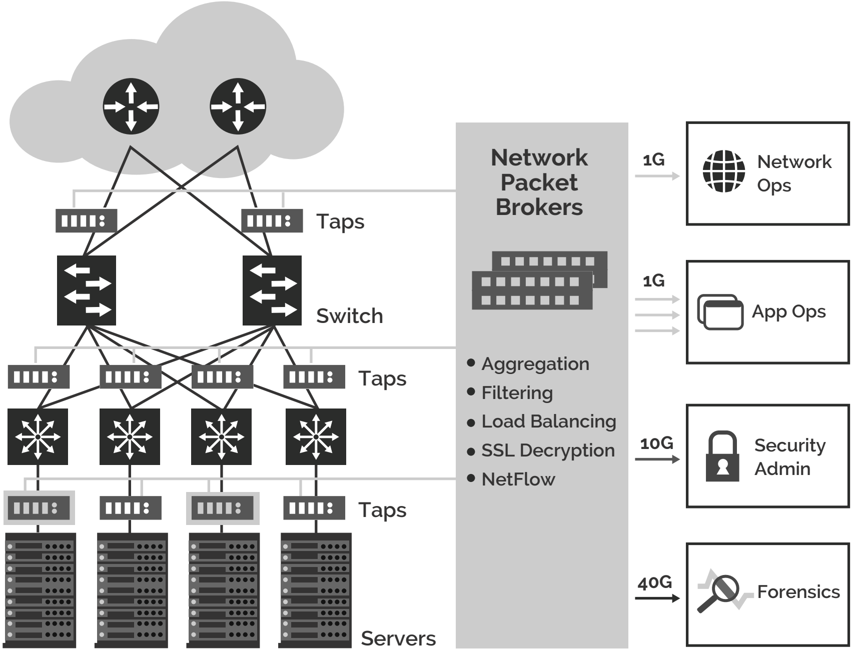


Figure 3-3: An intelligent visibility solution

But, here's the thing: Everyone claims inclusion of these intelligence features in their products. And, to be honest, they probably do have these features; but, there may also be a nasty little surprise awaiting your discovery. Make sure you read the fine print, because, while many products include such capabilities, they might not be supported for simultaneous enablement. So, if you need Netflow, SSL decryption, and time stamping all at once, you may be out of luck (or out of a ton of money that you spent on a solution that requires you to buy a lot of hardware).

It Is Precise

In 2005, one million pieces of malware were launched against unsuspecting victims over the course of the year. By 2015, one key fact about that statistic had changed: Rather than 1 million pieces of malware launched over the course of the year, that's the number of malware attacks that were launched *each and every day* of the year. Between malware and distributed denial of service (DDoS) attacks, your security solutions are inundated with alerts. What if someone on your security team needed to track these attacks down one at a time? Besides being *suuuuper* boring, the sheer magnitude of the manpower needed to follow up on millions of attacks per year would be beyond staggering. It would make the accomplishment of the Apollo moon missions seem like child's play. On the other hand, if you could just get rid of the confirmed bad traffic, would you just block it without even engaging the firewall?

Delegation is important! If you work for a micromanager, you know how frustrating it can be when he or she jumps in and attempts to do your job… and is terrible at it! Likewise, the visibility layer is not supposed to engage in deep packet inspection or perform in-depth analysis functions. Those are the jobs of the firewall and other security tools. Of course, if you knew in advance that certain traffic was bad, you would be wise to save your firewall inspection processing cycles by just chucking the bad traffic out the window immediately. The only way to accomplish this feat is to have access to a threat intelligence feed that tracks known bad IP addresses so they can be proactively blocked.

Imagine, if you will, a world in which you could isolate sources of known bad IP addresses and/or block entire regions of the world where you don't do business. You would massively reduce the number of security information and event management (SIEM) alerts your team receives. You'd be like the Superman or Wonder Woman of the SIEM world! That would be like reducing the noise in a crowded room or pre-sorting out the junk mail. With the clutter filtered out, you could better listen to the conversations that actually interested you, and you could focus on just the mail that actually required action. Think of what that would do to increase the efficiency of the rest of your security tools!

It Is Proactive

The best defense is a good offense. No matter your game, it is never won on defense alone. Instead, you need to get ahead of things a bit by playing a strong offense that provides you with a buffer in case things go badly for a while. So, while being reactive is important, being *proactive* keeps you in a power position. With proactive tools, you are made aware of *potential* problems immediately so you can fix them or even prevent them from becoming *actual* problems.

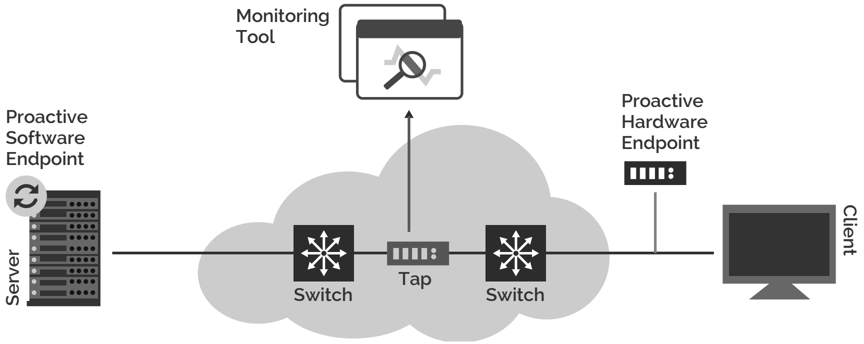


Figure 3-4: Proactive Monitoring using both software and hardware active endpoints

The drive to software as a service (SaaS) for many applications and remote distributed operations means that you have an increasing number of sites to monitor. For each tool and platform, you probably have service level agreements (SLAs) in place. If you could monitor those sites and platforms proactively, you could ensure that operations are running smoothly and meeting SLA guidelines. That would be a major advantage for a visibility system – proactively monitoring the current environment to make sure things are running smoothly at every remote location.

This may sound harsh, but when it comes to monitoring the systems your customers use, what you think doesn't always matter. Instead, the customer experience is of primary importance. Customer experience monitoring—looking at services from the perspective of your customer, rather than from your own perspective—is vital for a wide range of real-time applications, such voice tools, video, web services, and other critical enterprise applications. The goal is to ensure that the infrastructure delivers an amazing customer experience around the clock, even when there is no user traffic on the network to monitor.

Typical deployments consist of software and/or hardware active endpoints, emulated application traffic, and a simple web-based management and monitoring interface.

Once in place, you should be able to monitor SLA and customer experience, site-to-site and site-to-data center. You could monitor reliability and performance as well as perform proactive fault detection and isolation. You might even be able to conduct service readiness assessments and new service turn-up verifications. In other words, make a data-driven decision around new services rather than just throwing them in and hoping for the best.

What Are the Critical Features of a Visibility Solution?

Whether you already have a visibility solution or you're shopping for an upgrade, there are five critical elements you should look for – each of which is described in the following sections.

Network Packet Broker (NPB) Design

Network packet brokers are intelligent data distribution devices used to access and transform data into a format that security and network analysis tools can use. Basic data handling features such as deduplication and load balancing are important, but the devil is in the details. As you review solutions, make sure you look at *real* data throughput rates. For example, the spec sheet might say that it supports a whopping 40 Gbps of throughput, but what happens if you actually try to cram that much data into it? Can it actually keep up or will it simply collapse under the load? Also, make sure you know what happens when you turn on your entire wish list of features simultaneously. Does it light up, or does it blow up? And, of course, we need to ponder the real and profound problem of potential packet loss. You may just assume that your NPB distributes all of the incoming data, but does that really happen?

Well…

Zero Packet Loss

Let's say you push more data to your NPB than it can handle. There are a couple of considerations here. What exactly is that breaking point and, perhaps more importantly, what happens when you hit that point?

These are pretty important details! You should find the answers because they may surprise you, and not in a good way. If your NPB starts dropping packets when it is under real pressure, then it is, as we say in the industry, "not very good."

Deduplication

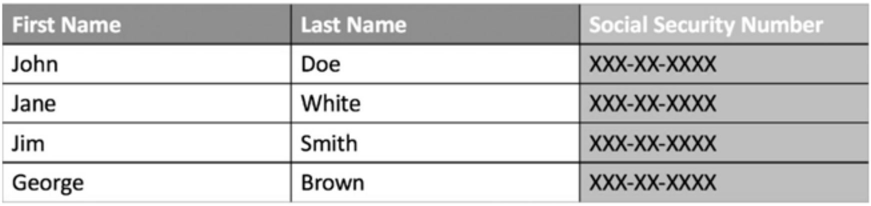
You learned earlier that network analysis and security tools commonly receive duplicate packets simply because SPAN ports frequently send multiple copies of the same data, or because data from multiple network taps are forwarded to the same tool. The NPB must eliminate all of the duplicate copies without losing any original data. Avoiding data loss: What a novel concept!

It is a basic function of the NPB that it should be able to accomplish *at its full specified data rate*. What good is a 40 Gbps NPB if it can't even achieve 30 Gbps once you turn on deduplication?

Data Masking

If you deal with personal data of any kind—and who doesn't these days?—then you have an obligation and requirement to protect that data. Bad things happen when you fail to do so.

When you send data to tools for analysis, you may need to strip out or mask sensitive data. As shown in Figure 3-5, your NPB should be able to perform this function without breaking a sweat, and do so regardless of which other features you have activated.



First Name	Last Name	Social Security Number
John	Doe	XXX-XX-XXXX
Jane	White	XXX-XX-XXXX
Jim	Smith	XXX-XX-XXXX
George	Brown	XXX-XX-XXXX

Figure 3-5: A simplified example of data masking

Programming and Management

Everyone claims that their product is easy to use. Some are. Others... well... not so much. Back in the olden days, everyone thought their fancy MP3 digital music players were all the same until Apple introduced the iPod and redefined the concept of 'ease of use.' There are a lot of similarities here. When you set up rules and connections in the NPB, intelligence matters a lot. If you need a PhD in Boolean logic programming to understand how to program your NPB, chances are pretty good that mistakes will be made; unless, of course, you actually have a PhD in Boolean logic. (Hi, Bob.)

A lot of complexity is introduced because of an overreliance on command line interfaces (CLIs). The issue with programming exclusively via CLI is that each connection's statement must be logically correct. If it is not, then you have probably just programmed a connection that goes nowhere, much like a once-planned bridge in Alaska. Worse, you may not even get an error, so while you think you just connected a data source to your firewall, the connection was invalid, so that data is simply bypassing the firewall altogether—and you have no idea.

Simpler is always better, and having a drag-and-drop interface that automatically validates and deconflicts connections makes programming much faster, more intuitive, and much less prone to mistakes.

Nice, eh?

Why Bother With All of This?

Why pay any attention to visibility? It's the foundation to operationally ensuring your network is running as it should. It is what delivers data to all of your security and analytics tools.

The better you load-balance your traffic, the more life you can get out of your existing tools. For instance, if you have multiple 10 Gb firewalls, each protecting different parts of your network, and your throughput needs have exceeded their capacity, you can load-balance across them instead of throwing the firewalls away and upgrading to the next higher speed.

There are some additional benefits as well:

- Decreased downtime for troubleshooting and lowered Mean-Time-to-Resolution (MTTR)

- Increased reliability, performance, and security
- Expanded ability to meet regulatory compliance for external audits
- Significant ROI because a better foundation leads to better use of existing tools, faster troubleshooting, overall less downtime
- Reduced security costs through more efficient use of tool resources
- Increased uptime for security resources protecting the network
- Improved SLA compliance
- Easier application, data center, and cloud reliability and performance monitoring
- Faster deployment and fewer misconfigurations for new service and application rollouts

Next Steps

In the next chapter, you'll learn in more detail about taps, bypass switches, and NPBs. You'll find out why you would use them, and how they can help you provide the ultimate visibility to your organization.

4

Selecting the Ideal Visibility Solution

Okay, perhaps by now you are thinking, ‘is this topic of visibility *really* all that serious?’ If you’ve been reading this book from the beginning, you know just how serious it can be – especially if you get it wrong. And at least now you have a fighting chance to identify what matters in your specific network and identify a solution that offers total visibility.

You rate your servers and storage on more than just their performance and availability specs. Visibility is no different. In addition to speed ratings and number of ports, the network packet broker design should also be able to meet speed requirements with zero packet loss, have resilience and failover options, and provide packet processing intelligence to empower your security and analytics tools.

In this chapter, we will look at a set of network taps, bypass switches, and network packet brokers from one company, Ixia, and show how they do more than just what is on their spec sheets.

Visibility Taps

If you don’t already have a variety of network and security systems that all need access, you will. More locations, more data throughput, more clouds, and more devices all add up to more locations you need to pull data from. That access is obtained by using a network tap (or “visibility tap,” as they’re often called) in order to gain that non-intrusive, or passive, access to the data flowing across the network.

Taps are usually placed between any two network devices (including switches, routers, and firewalls) to provide network and security systems a view into the network.

Once a tap is in place, protocol analyzers, remote monitoring (RMON) probes, and intrusion detection and prevention systems can be easily connected to, and removed from, the network as needed, and with no downtime.

Network and security devices that are connected to a tap receive a mirror of all network traffic flowing across that link, including any and all link layer errors. It’s a lot of data but you need it all-at-once, so you better make sure you are deduplicating it before it hits your tools (Hint: that is one of the jobs of the NPB).

One of the great things about using taps is that they don’t introduce network delay, alter the content or structure of the data, or provide a point of failure (they fail open so that if the tap loses power or monitoring devices are disconnected, network traffic is uninterrupted).

Visibility Taps vs. Traditional SPAN Ports

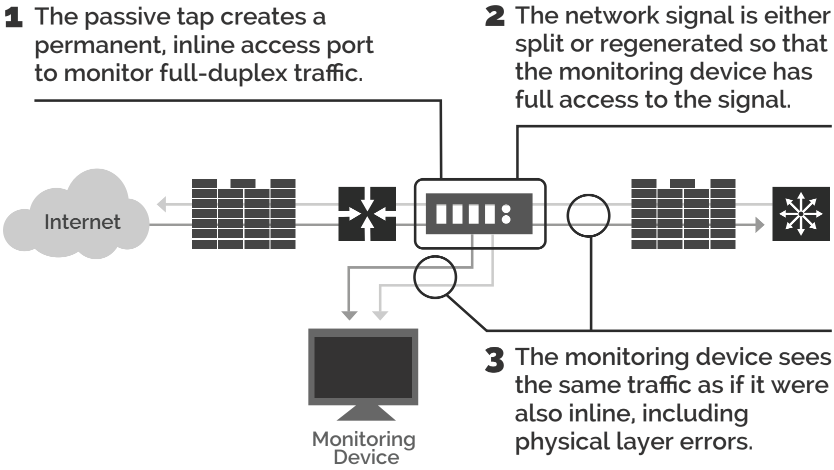
We talked about the benefits of taps over SPAN ports in previous chapters, but let’s summarize the differences here:

- SPAN ports require an engineer to configure the switch, or switches; taps do not

- Switches can eliminate corrupt packets and send modified packet streams through SPAN ports; taps do not

- SPAN ports can be easily overrun by large data streams, as mirroring is a low priority task for a switch; taps do not exhibit this shortcoming

The example shown in **Figure 4-1** illustrates a typical tap deployment for one monitoring device.



1 The passive tap creates a permanent, inline access port to monitor full-duplex traffic.

2 The network signal is either split or regenerated so that the monitoring device has full access to the signal.

3 The monitoring device sees the same traffic as if it were also inline, including physical layer errors.

Figure 4-1: Typical tap deployment for one monitoring device

Ixia's Tap Family

Ixia has a broad and comprehensive portfolio of network taps. As a part of a complete end-to-end visibility architecture, the network taps feed network packet brokers. Regardless of interface or location in the network, Ixia has a tap solution: From copper to multimode/single mode fiber, at speeds up to 100Gbps with media conversion models, and of course, virtual taps. For any visibility solution you're considering, make sure that you're able to procure any and all taps that you might need.

Taps are great if you want to access data, but if you want to place security tools inline safely, you need a really good bypass switch.

Bypass Taps (Bypass Switches)

Placing any device inline has its risks, but if you are dealing with security, you cannot afford to place it out-of-band. If you take security seriously—and who can afford not to? —you will need to go inline with your security systems. And if that appliance stops working—or just has to be updated, which they **all** do at some point—then suddenly your network traffic, well... just stops. To put it mildly, that is not good.

The way to solve this is to use a bypass switch to provide fail-safe protection. Whether you are deploying inline security and monitoring devices, such as a firewall, an intrusion prevention system (IPS), web application firewalls (WAFs), or anything else critical to protecting your network, a bypass switch can save you. (**Figure 4-2**).

Figure 4-2: An iBypass VHD unit from Ixia

A good bypass can fail open or closed. It can be programmed with an intuitive drag-and-drop GUI rather than a cumbersome logic table, and it can be a stand-alone device. All-in-one NPBs with integrated bypass switches sound cool when you first hear about them, but when you look at the numbers—as we did in chapter 3—you see quickly that having these platforms separated makes way more sense. Every time you want to upgrade, maintain, or outright replace one of your inline devices, a bypass switch means never having to say the network is down. That is good.

Ixia offers a wide array of iBypass switch products that handle different high availability features, speeds, and media types. Look at their iBypass VHD platform to see how many of your requirements you can check off.

Network Packet Brokers (NPB)

You have now tapped in to all of your data and you have a bypass for resilience. It is time to distribute all of this data to either your inline security tools or your out-of-band analysis tools. And while we would love to believe that all of your data resides in one place, it is far more likely that your data is hosted across multiple locations and multiple clouds, meaning you have more than one distribution problem to solve.

A network packet broker (NPB) is a device that provides smooth data distribution across all of those security and monitoring tools. Remember the old images of 'Mabel at the switchboard' manually connecting telephone calls back in the 1960s? That is not the world you live in. You have too much data coming from too many sources, moving far too quickly. The modern network needs a data distribution system and the network packet broker—or visibility device—is that engine. The word *broker* is helpful to focus on here.

Figure 4-3 shows how an NPB receives data from a number of network links. NPBs are active devices "brokering" or "distributing" data to the relevant monitoring tools.

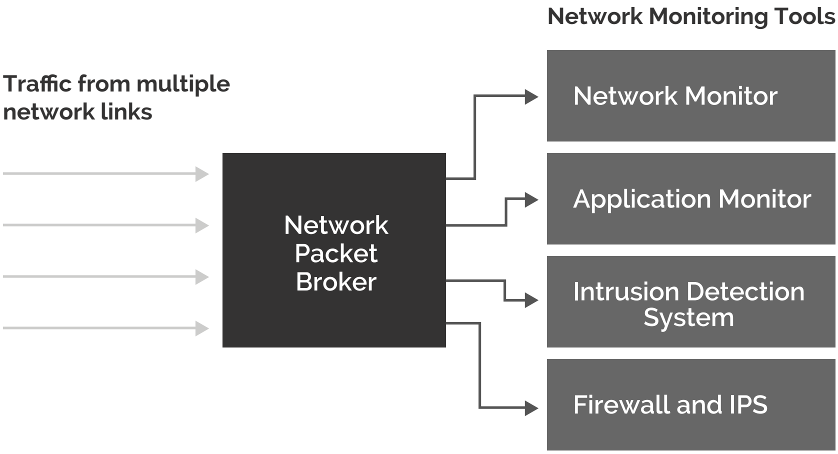


Figure 4-3: Illustration of a Network Packet Broker in action

In its simplest actions, the NPB can:

- Deal data from one network link to one tool.
- Deal data from one network link to multiple tools.
- Deal data from multiple network links to one tool.
- Deal data from multiple network links to multiple tools.

However, it is the more advanced features that will determine exactly how stable and how insightful your network tools are. Whether your networking tool is a firewall, IPS, compliance system, forensics device, or something that performs data/application analysis, it will only be as good as the data it receives.

So what are the advanced features that you need to look at in an NPB?

It's important to remember that NPBs aren't all created equal. There are at least four things you need to make sure your NPB can do.

1. **Data Deduplication at Production Rates**
   When you tap in to data from multiple locations, you are going to get data duplicates. Sending the same data twice into your networking tools—especially with slightly different time stamps—will quickly mess up their performance. Duplicate packets must be removed before reaching monitoring and security tools. During this process, it's imperative not to accidentally drop any original data.

   Advanced NPBs offer zero-loss advanced packet processing at full line rate. Just because everything works great in a lower volume proof-of-concept (POC) doesn't mean it will do as well when you scale up to production rates.

2. **Resilience**
   Choices are not just good; they make the difference between whether or not your network will handle the unexpected. And the unexpected is bound to happen. For instance, you may be load-balancing between two active firewalls, or you may have a failover 'hot spare' redundant path you put in place in case of failure. You need to know your network can immediately handle either situation.
   Accomplishing this requires not just programmability but also heartbeats, so you can constantly monitor the availability of every tool, all the time. So as long as you have a heartbeat where you can check the status of every tool, you are covered, right? Well, not so fast... or maybe faster.

   If your network has strict latency and uptime requirements, then heartbeats every few seconds may be way too slow; heartbeats every second may not be fast enough; it's even possible that hundreds of milliseconds won't do it. You may need a few milliseconds or even microseconds.

Looking at Ixia gear, we see that they have the industry's fastest heartbeats, which go down to nanoseconds. When it comes to meeting the needs of your network consumers, having options to know instantly when one tool is down, and implementing routes around it in far less than a second might be exactly what you require.

3. **Application and Security Intelligence**
   Troubleshooting speed is driven by how much you know. Large networks can have hundreds of applications running, especially with the growth of "bring your own device" (BYOD). Intelligent NPBs can identify the applications in use on the network and provide that intelligence to any of your tools.

   Many tools in use only need to monitor or inspect specific types of applications. Intelligent NPBs can easily deal traffic out to monitoring and security tools via application flow. This makes your monitoring and security tools much more efficient, and it makes life much easier for administrators.

4. **Simultaneous Features**
   If you have a lot of analysis tools on your network, you are going to need to use a lot of data conditioning features. For instance, if you are running forensics on your data, you will want precision time stamps on every data packet. If you deal with any kind of personal information, then you will need to verify compliance and ensure you are meeting specified data masking requirements. That means when you send data up to your tools, you have masked any personal data.
   Okay, one more: If you are troubleshooting, you will want to be able to recognize which data streams are coming from which applications, where those streams originated, and what device they are accessing. This will save immense amounts of time in

troubleshooting issues. For example, it can tell you that a user is accessing Facebook on an iPhone from New York City.

So, if we start with deduplication and add time stamping, data masking, and application intelligence, how well does the packet broker now handle data load? It turns out that a lot of packet brokers do not even support using all those features at once. If you want all those features, you need to buy additional packet brokers or additional modules.

Ixia is capable of providing all of those features simultaneously, without even breaking a sweat. And best of all, they handle multiple features better than anyone else we've found because they use hardware processors to handle specialty features, rather than using slower network processors.
Hardware processors are critical if you want to use your shiny new network packet broker in your production environment. If your network packet broker uses a common network processor, be ready to buy more than one if you want to keep up – and there goes your budget and ROI.

5. **Security Intelligence**
If your visibility layer can help your security tools do their jobs better, then you want to take advantage of that. There are some advanced NPB features that really do make a difference. The first is SSL decryption. You want to make sure that all of the incoming data is properly routed and properly inspected. The only way to know this is if it is unencrypted. Your NPB should have this feature.
One very advanced feature Ixia products are capable of is the leveraging of an application and threat intelligence feed. For example, if you are a university setting and you feel confident that Netflix traffic, for instance, poses a minimal security threat,

you might want to allow it to bypass the firewall – assuming the feed is authentic. An application intelligence feed can validate the server source and other attributes to ensure it is coming from an authentic Netflix server. This one example would save lots of firewall processing resources.

A great solution allows you to also filter out all *known* bad IP traffic so that you can conserve firewall resources Ixia's Threat-ARMOR product serves this function and blocks confirmed bad IP addresses, unregistered and hijacked IPs, and is fed from its own threat intelligence feed. As part of an overall visibility solution, this one feature can drop security events by as much as 80 percent. That would take a big burden off of both your security tools and teams – allowing them to focus on the rest.

Next Steps

So now you've learned what visibility is, how to know if you need more visibility, and the limitations of common tools. You also learned:

- What features to look for when selecting new visibility solutions;

- What makes for a successful visibility implementation;

- How taps, bypasses, and network packet brokers are critical to total visibility,

- And, that visibility and security go hand-in-hand.

To learn more about how Ixia can bolster your visibility capabilities, visit **http://www.ixiacom.com/enterprise**.

Discover true visibility and how the right solution improves security and brings the entire network into view

Network security mishaps and performance problems are daily occurrences around the world. At the same time, businesses become more dependent on their data centers and network infrastructure with each passing day. The only way to stay ahead of the endless adversity that threatens your organization's IT infrastructure is to have complete and reliable network visibility. In this book, you'll learn what true visibility looks like, and will discover how to provide your company with an unmatched level of visibility that can bring more secure and responsive results.

In This Book:

- Find out what visibility is any why you need it in the first place
- Discover the components that make up a great visibility platform
- Learn how to tell if your current visibility capability is really meeting your needs

ActualTech Media
For bonus content & more
Visit **www.ActualTech.io**

Not for Resale
ISBN 978-1-943952-15-1