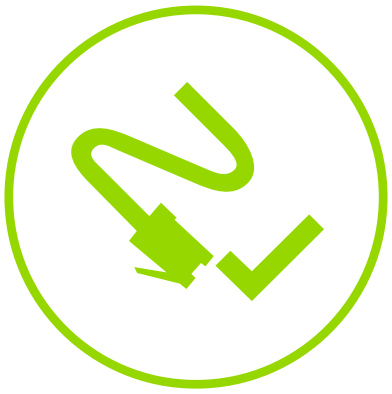


Solving the Challenges of Packet Captures

Accelerating root cause analysis with Profitap & NetAlly

White Paper

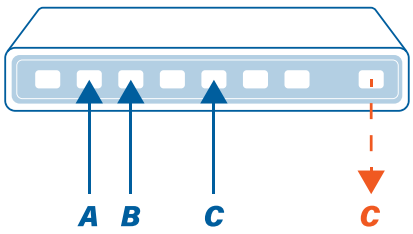
The first step in successful packet analysis for root cause troubleshooting is to capture the right packets – the ones that contain the evidence needed to resolve the issue. In this white paper, learn how the combination of tools from Profitap and NetAlly simplify getting access to the packet data.

In many cases, network problems can be resolved through SNMP statistics and active or throughput testing. However, there are times when the only way to get to the root of a problem is through packet capture. During those times, it is critical to have the best tools to ensure you are capturing all of the necessary packets. Without all the packets, it can be difficult — if not impossible — to get to the root of the problem. This is where the combination of the NetAlly EtherScope™ nXG and the Profitap Booster In-Line are a perfect packet capturing solution.

There are several steps capturing and analyzing network traffic successfully. In this paper, we will examine each of these steps, and the role the EtherScope™ nXG and the Booster In-Line play.
The first step in any successful packet capture is getting access to the packet data. We cannot merely plug into any switch port and expect to capture the packets between two devices. There are several standard methods for getting in the path, each with their benefits and challenges. Let's take a look at three of the most common methods for getting in the path of the packets.

SPAN Ports

This is by far the most popular method for capturing traffic to a device connected to an Ethernet switch. Port spanning involves configuring the switch to copy all of the ingress and egress traffic on one port to another port. This allows the analyzer to be connected to the destination port and monitor the traffic going in and out of the source port.



Pros:

- Doesn't require the link to be broken
- Easy to configure
- Low cost, integrated into the switch
- Can be implemented quickly

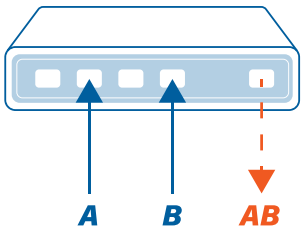
Cons:

- Aggregates the traffic into a single port
- Requires configuration access to the switch
- Configuration commands vary from switch to switch
- Not available on all switches
- Doesn't copy all packets (ignores certain types and sizes)
- Alters packet timing

For low bandwidth captures, the SPAN port may be a good solution. However, with a full duplex gigabit connection, it is possible that the ingress and egress traffic will exceed the 1 gigabit egress capability of the SPAN port. In this case, packets will be dropped, making the analysis process much more difficult. Making a change to a switch configuration may not be an issue in some networks, but large networks often require change control processes to be followed before the configuration of the switch can be changed. This can increase the time it takes to get in the path of the packets and begin resolving the problem.

Aggregation TAPs

Another means of getting in the path of the packets is an aggregation TAP. This is a device that is physically placed in the connection between the device being monitored and the rest of the network. The ingress and egress packets are aggregated into a single data stream and sent out a single Ethernet port.



Pros:

- No switch access is required
- Fault tolerant, if the TAP loses power, packets continue to pass
- Can be put in place during network construction

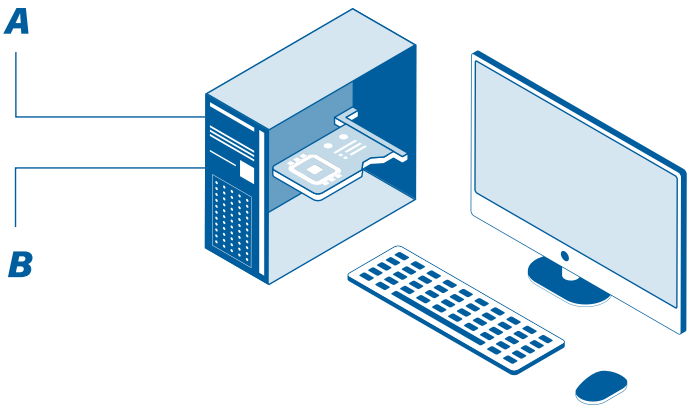
Cons:

- Easy to oversubscribe the output port
- Must break line to install
- Must be purchased

The aggregation TAP has the benefit of not requiring switch access. As with the SPAN method, aggregation TAPs can be easily oversubscribed, causing packet loss. In most cases, the aggregation TAP is a good solution when the analyzer is only capable of capturing network traffic on a single gigabit interface.

Computer with 10 gigabit NIC

One way to overcome the aggregation issue is to use a capture device with a network interface that exceeds the full duplex bandwidth of the link being monitored. A computer with a 10 gigabit NIC (Network Interface Card) is one approach. This allows the TAP to aggregate the traffic and send it out an interface that operates at a speed greater than the sum of the ingress and egress traffic.



This challenge with this solution is finding both a computer with a 10 gigabit NIC and the ability to capture at full line rate 10Gbps. In most cases, the computer will only be able to capture at a fraction of full line rate and write the traffic to memory or disk.

NetAlly EtherScope™ nXG and the Profitap Booster In-line

When it comes to getting in the path of the packets and perform lossless packet capture, the combination of the NetAlly EtherScope™ nXG and the Profitap Booster In-line is hard to beat. These two tools provide the ability to get in-line, capture on multiple links at the same time, and capture packets at full line rate 10Gbps.

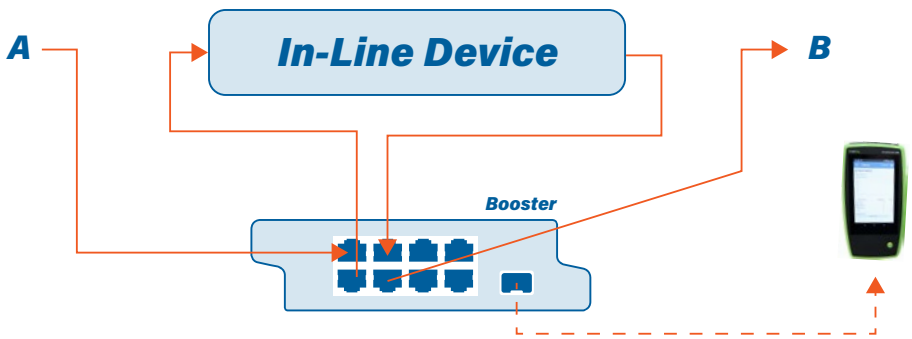
The Profitap Booster In-line features four fault tolerant in-line TAPs integrated into one small form factor. Each of these TAPs passes PoE, and fails to wire in case of power loss. Why is this important? We never want to put a monitoring device into the network that could cause an outage if the power should fail. If power fails on the Booster, it will continue to pass packets through each of the four TAPs.

The traffic from the 4 TAPs is aggregated and sent out a 1G/10G SFP+ interface. This interface accepts a variety of copper and fiber SFPs, as well as DAC cables. With a 10Gbps interface, even if all 4 TAPs are running at 100% in both directions, they only aggregate to 8Gbps, which does not exceed the egress speed of the output port.

As mentioned with trying to use a computer with a 10Gbps interface, it is not easy to capture traffic at full line rate 10Gbps. This is where the NetAlly EtherScope™ nXG comes in. The 1G/10G SFP interface on the EtherScope™ nXG is capable of capturing traffic at full line rate 10Gbps with no packet loss. This ensures that all packets that arrive at the interface are captured and available for analysis.

Capturing on both sides of a device

A question that comes up when identifying bottlenecks in the network is "how much latency is this device adding?" With a typical analysis solution, this is a very difficult question to answer. This is not the case when using the NetAlly EtherScope™ nXG and the Profitap Booster In-line. The Booster can be connected in-line both before and after the device being tested.



The packets going into and out of the device are aggregated and sent to the EtherScope™ nXG. This provides a way to accurately measure the latency of the device between the two TAPs. Once the latency is measured, it is possible to determine if the device is the cause of the bottleneck.

More than just a capture tool

The EtherScope™ nXG is more than just a packet capture tool; it is a powerful network discovery tool as well. Through the use of name discovery, SNMP queries, and Wi-Fi analysis, the EtherScope™ nXG is able to collect the names and address information of devices on the network.

This name and address discovery helps resolve another challenge faced when analyzing packet traces, which is correlating names with addresses. When looking through trace files, often times, only the IP address of a device is displayed. By associating a name with the device, the time necessary to get to the root of the problem is significantly reduced.

Remote access and trace retrieval

The analyst cannot always be at the same location as the network problem. The NetAlly EtherScope™ nXG and the Profitap Booster In-line can be deployed at a remote site and operated from another location.

Through the use of VNC or web remote control, the EtherScope™ nXG can be controlled as if the analyst was sitting right in front of it. This means that packet capture filters can be created, and the capture started, all without being at the remote location.

Once the capture is complete, it can be uploaded to NetAlly's Link-Live Cloud Service. Through the Link-Live web interface, the trace file can be downloaded an analyzed from anywhere. This allows the analyst to troubleshoot problems thousands of miles away, without the need to travel.

Summary

Capturing and analyzing network traffic successfully takes planning and the correct tools. While there are a number of ways to get in the path of the packets and capture them, it is important to understand the pros and cons of each. In the end, without all of the necessary packets, it is very difficult, if not impossible, to analyze and troubleshoot network and application problems.

The combination of the NetAlly EtherScope™ nXG and the Profitap Booster In-line achieves the following:

- Get in the path of the packets
- Pass PoE
- Aggregate network traffic, without oversubscribing the output port
- Capture at full line rate 10Gbps
- Discover device names and addresses
- Operate analyzer remotely and retrieve trace files through Link-Live

This professional-class packet capture setup ensures that the analyst can get the right packets the first time and reduce the time to resolution.

For more information on the EtherScope nXG visit: www.netally.com/products/etherscopenxg/
For more information on the Profitap Booster In-Line visit: www.profitap.com/booster-inline/