Troubleshooting 100G Ethernet Using Filtering and Packet Capture

Mai Abou Shaban, Product Manager, Transport Business Unit

With 100G set for mass deployment in order to address the growing demand for bandwidth, service providers and network operators are facing a number of challenges. Some of these challenges are related to the multiservice offering of 100G networks, the nature of each and every one its supported services, and its implications on SLAs. And, as the service offering scales to the 100G rate and becomes more complex, network engineers are being called on to perform even more troubleshooting and service calls.

100G network troubleshooting involves performing a number of complex procedures to identify where and why network failures are occurring. Network engineers usually have very little information about the event, and must investigate various probable causes of failure. The difficulty of these tasks is compounded by the pressure of having limited investigation time and the risk that customers will be affected.

Of the options at their disposal, network engineers have the ability to capture the traffic on the affected circuit and decode it. Decoding traffic usually involves analyzing the content of the header to identify any issues, such as modifications or incorrect content.

In order to ensure the proper deployment and optimal performance of 100G Ethernet networks, it is imperative that carriers use the right tools for troubleshooting. This application note describes EXFO's FTB-88100NGE Power Blazer, a 10M-to-100G multiservice testing solution, and its unique 40G/100G Ethernet advanced filtering and capture that make it the tool of choice for 40G/100G field testing.

The FTB-88100NGE Ethernet capture tool offers the following advantages:

- Powerful Ethernet capture/decode capabilities, along with 10M-to-100G Ethernet test capabilities, including EtherBERT, RFC 2544 with Smart Loopback, Traffic Generation and monitoring all on a single compact module designed for field testing.
- Industry-standard capture files in packet capture (PCAP) format, with decoding capabilities performed via Wireshark, an industry leader and the de facto standard in packet analysis and decoding.
- Ethernet capture is performed directly from the 40G/100G C form-factor pluggable (CFP) test port of the FTB-88100NGE Power Blazer module, eliminating the need for additional hardware and reducing the number of failure points in the test architecture.

The FTB-88100NGE Power Blazer's supported Ethernet capture offers essential capabilities to increase network engineers' efficiency and reduce downtime. These capabilities include comprehensive filtering and triggering methods to target specific traffic and capture what matters most.

FILTERING

In most troubleshooting situations, the focus is on one particular traffic stream, while the rest of the traffic is able to consume memory without providing any useful information. The FTB-88100NGE capture tool provides the ability to filter Ethernet traffic in order to capture only traffic that fits a specific profile, therefore efficiently using the available memory.

The filter engine is based on basic and advanced filtering capabilities. In the basic mode, the user can filter traffic based on a single trigger value, while the advanced mode provides the ability to customize a filter using up to four triggers combined with logical operands (AND, OR, NOT). In both cases, a complete set of triggers is available, including MAC, IP, UDP and VLAN.

TRUNCATION

In most captures, the payload information is typically proprietary information that cannot be decoded by the test equipment. As such, network engineers usually focus on the header information, which is decoded and used for more in-depth troubleshooting. Again, this eliminates the capture of unnecessary data that would otherwise consume memory without providing any additional useful information.

The FTB-88100NGE provides an innovative truncation capability that limits capture to a specific number of bytes, starting from the first bit of the Ethernet frame. Network engineers can therefore limit capture to the first few bytes of the header, or add more bytes to include higher-layer information.

CAPTURE TRIGGERS

A very common issue with typical capture tools is that capture starts as soon as the capture tool is enabled. However, the event of interest may occur later, allowing previously captured traffic to fill the memory buffer without providing any useful information. In some cases, the testing opportunity can be completely missed due to the high amount of captured data and the short event window.

EXFO's Ethernet capture tool solves this issue by including a set of triggering capabilities that allow customers to fine-tune and specify when the capture process should start. This powerful capability simplifies the troubleshooting process by filling the memory only when the event of interest is detected. The memory and the troubleshooting time are therefore efficiently used, resulting in meaningful capture data that yields more important information.

Users can capture traffic based on the following three types of triggers:

- **Manual Trigger** is the simplest form of trigger and basically starts the capture as soon as it is enabled. This is the default mode of operation that mimics traditional capture tools.

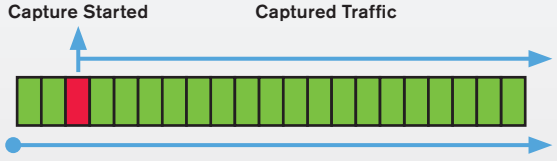

Figure 1. Manual Trigger

- **On-Error Trigger** is a trigger that starts to capture the operation when a specific event is detected. These events are typically Ethernet errors such as frame check sequence (FCS) errors. This mode enables on-event capture, a scenario where a capture device monitors the circuit until the specific event is detected and the capture is triggered.
- **Field-Match Trigger** launches the capture when a frame with a specific filtered condition is detected. This condition uses a system similar to the traffic filter system and enables the user to monitor the circuit and start the capture as soon as a specific frame condition is detected.

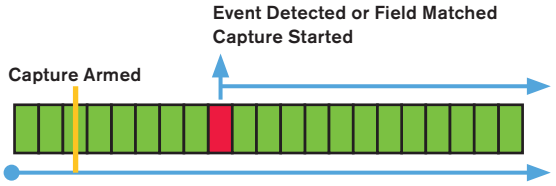

Figure 2. Field-Match Trigger

TRIGGERING POSITION

The triggering position is used to determine the position of the triggered frame within the captured data, solving a common problem with traditional capture tools, whereby the event of interest is often located within the capture data.

A typical use for the triggering position is to perform pre- and post-analysis. In network troubleshooting, it is very important to understand the events that led to the failure and to view the events that followed the failure. These two critical phases provide a wealth of information about the failure, what caused it, and how the network reacted to it.

The triggering-position capabilities allow the user to specify where the trigger event will be located in the capture, making it possible to select the frames to be captured depending on their position relative to the trigger event. Traditional capture tools do not offer the ability to perform a mid-trigger or pre-trigger; instead, they only provide post-trigger capabilities. As such, users are left to manually search within the captured sequence to identify the event and perform the analysis. This, in combination with the lack of a trigger mechanism, means that it is possible to completely miss the event of interest when using traditional capture tools, resulting in an inefficient capture process.

EXFO's Ethernet capture tool provides three triggering positions, as follows:

• Post-Trigger

In Post-Trigger mode, the first frame of the capture is always the trigger, and the remaining frames are the frames that follow the trigger event. This mode is typically used to analyze content after the event.

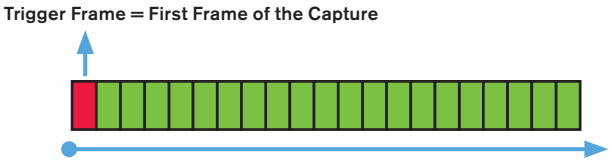

Figure 3. Post-Trigger

• Pre-Trigger

In Pre-Trigger mode, the last frame of the capture is the trigger event; therefore, the captured output contains all the frames leading up to the event. This mode can be used to determine what led to the specific event.

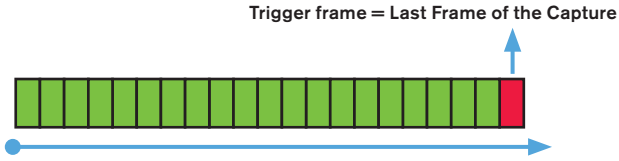

Figure 4. Pre-Trigger

• Mid-Trigger

Mid-Trigger mode is a very powerful application that provides a snapshot of the traffic before and after the trigger event. In this mode, the trigger event is usually in the middle of the captured traffic.

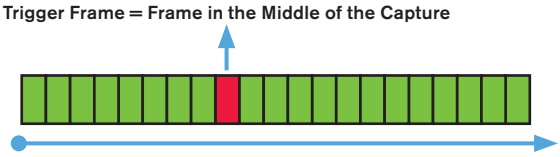

Figure 5. Mid-Trigger

EXPORTING CAPTURE AND ANALYSIS

Once a capture is completed, the captured data can be exported to the platform's internal memory for decoding. The exporting process generates an industry-standard PCAP file that can be used by a variety of open-source decoding tools. Decoding and post-analysis is performed using the Wireshark application.

CONCLUSION

With 100G moving toward mass deployment, the FTB-88100NGE Power Blazer's Ethernet capture and decode capability allows network engineers to quickly pinpoint issues in the field and speed up the troubleshooting process to ensure quick service recovery.

EXFO Headquarters > Tel.: +1 418 683-0211 | Toll-free: +1 800 663-3936 (USA and Canada) | Fax: +1 418 683-2170 | info@EXFO.com | www.EXFO.com

EXFO serves over 2000 customers in more than 100 countries. To find your local office contact details, please go to www.EXFO.com/contact.

APNOTE282.1AN © 2013 EXFO Inc. All rights reserved. Printed in Canada 13/03

EXFO | Assessing Next-Gen Networks