

Troubleshooting Ethernet Services with Packet-Capture and Decode Capabilities

By Thierno Diallo, Product Specialist, T&D Business Unit

Ethernet networks have experienced incredible growth in the amount of data that they carry. With increased reliability, Ethernet networks have transitioned from being pure Ethernet data pipes to carrying Ethernet services. Ethernet commercial services now carry triple-play services for enterprise and commercial customers, while mobile backhaul networks now carry time-sensitive and mission-critical data services across packet networks, enabling mobile convergence. As the service offering becomes more complex, network engineers and field technicians are required to respond to more troubleshooting service calls that require them to rapidly pinpoint, analyze and report quality of service issues.

Network troubleshooting involves performing a number of complex procedures to identify where and why a network failure is occurring. While network technicians and engineers usually have very little information about the event, and they must search through multiple possible causes of failures. What's more, the task becomes even more difficult with the pressure of having limited investigation time, in addition to knowing that customer's may be greatly affected.

Among the many tools available to the technician, a very popular one is the ability to capture the traffic on the affected circuit and to decode it. Decoding the traffic usually refers to the interpretation of the content of the header to identify any issues in the content of the header, such as modifications and incorrect content. Decoding also allows investigators to identify the true content of the circuit as all the traffic, such as customer traffic and network command-control traffic, is captured. A technician can then search through the list of packets and identify out-of-place or inconsistent traffic by analyzing the overhead content of the captured traffic.

This article offers insight into troubleshooting Ethernet services with the implementation of EXFO's new packet-capture and decoding capabilities.

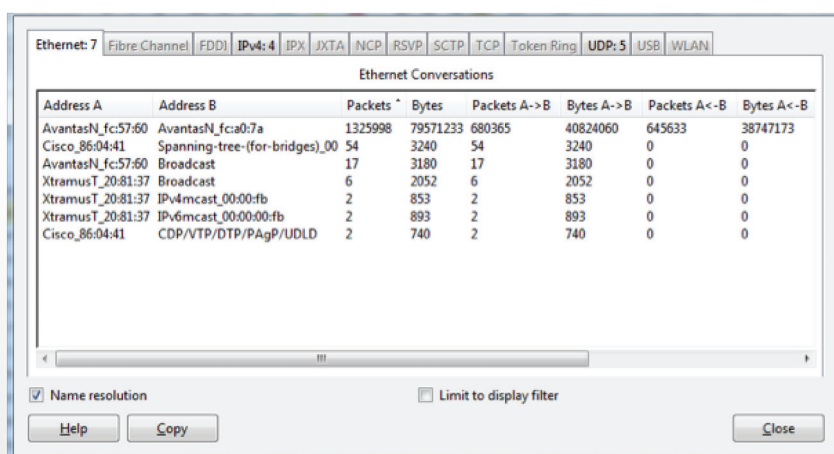
FIELD APPLICATIONS

Although portable test units can provide powerful test capabilities, there are a few situations where packet capture can provide more information for enhanced troubleshooting. Here are a few examples:

Top-Talker Analysis

A typical issue with network operators is identifying those who monopolize the bandwidth, i.e., stations that consume too much bandwidth and users that engage in heavy download, illegal streaming or even virus-infected computers. From a carrier perspective, the monopolization of bandwidth can indicate congestion or incorrect configuration of transport devices.

A packet-capture session can complement troubleshooting by capturing the actual content of the pipe as the issue occurs. Offline analysis can then provide bandwidth and utilization statistics, such as top talkers (MAC, VLAN and IP) or packet distribution.



The screenshot shows a software window titled 'Ethernet Conversations' with a tabbed interface. The 'UDP: 5' tab is selected. The window displays a table with columns: Address A, Address B, Packets, Bytes, Packets A->B, Bytes A->B, Packets A<-B, and Bytes A<-B. The table lists several network conversations, with 'AvantasN_fc57:60' and 'Cisco_86:04:41' showing the highest traffic volumes.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
AvantasN_fc57:60	AvantasN_fc57:60	1325998	79571233	680365	40824060	645633	38747173
Cisco_86:04:41	Spanning-tree-(for-bridges)_00	54	3240	54	3240	0	0
AvantasN_fc57:60	Broadcast	17	3180	17	3180	0	0
XtramusT_20:81:37	Broadcast	6	2052	6	2052	0	0
XtramusT_20:81:37	IPv6mcast_00:00:00:fb	2	853	2	853	0	0
XtramusT_20:81:37	IPv6mcast_00:00:00:fb	2	893	2	893	0	0
Cisco_86:04:41	CDP/VTP/DTP/PAGP/UDLD	2	740	2	740	0	0

At the bottom of the window, there are checkboxes for 'Name resolution' (checked) and 'Limit to display filter' (unchecked), along with 'Help', 'Copy', and 'Close' buttons.

- › An analysis tool can provide the statistics per conversation and identify those who monopolize the bandwidth.
- › Top-talker analysis is performed by sorting the analyzed statistics.

Performing Deep-Packet Inspection

The three main configuration issues with packet-forwarding devices is fragmentation of the traffic, VLAN tunneling and the header fields overwrite:

- Traffic fragmentation occurs when a device must segment the traffic into smaller sizes in order to transmit within the maximum transmission-unit limit of a pipe, i.e., the maximum data size allowed in a pipe. When fragmentation occurs, performance is typically reduced as less effective bandwidth is available with the increased frame numbers required to transmit the same data size.
- Tunneling occurs typically when an Ethernet device adds, swaps or removes VLAN tags as it processes traffic. Tunneling typically occurs at the edge of the network where untagged traffic is first tagged then forwarded on to the L2 network or when tagged traffic is untagged and forwarded to the proper destination.
- Header overwrite sometimes occurs when traffic with a specific priority, usually IP TOS/Diffserv, is forwarded with a different priority, causing QoS issues during congestion.

In these three cases, capture provides a real-time view of the issue and allows network investigators to perform deep-packet inspection using the overhead decode capabilities.

Troubleshooting the Customer's TCP Issues

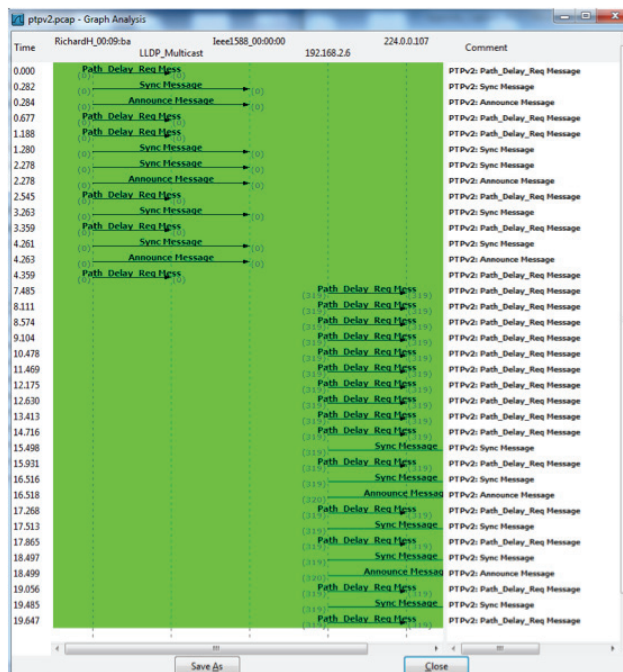
Although EXFO's TCP application provides significant service turn-up testing of TCP pipes, troubleshooting the customer's TCP issue requires testing on the actual customer's TCP streams to identify overhead or connection issues.

The packet-capture capability complements TCP testing by providing capture and decoding analysis of the customer's actual TCP exchange. Decoding provides insight into the content of the overhead and provides further sequence analysis such as providing a graphical flow of the exchange and identifying retransmission and duplicate acknowledgements. By using a decode capability, the user can therefore analyze the events leading to the duplicate or retransmission and also ensure that the proper retransmission has occurred after the event.

New Services Analysis

In addition to VoIP and video (IPTV), carriers are now implementing Ethernet-synchronization services, especially for mobile backhaul. Precise Time Protocol (IEEE1588 PTP) is a new protocol designed to establish and maintain synchronization in a packet network based on a client-server architecture, where client boundary clocks maintain clock synchronization and stability using notification and requests from a master clock.

Packet-capture and decode capabilities provide a simple and intuitive approach by enabling the capability to capture these services and perform conversational and deep-packet analysis, identifying conversation issues, such as packet loss and incorrect sequences.



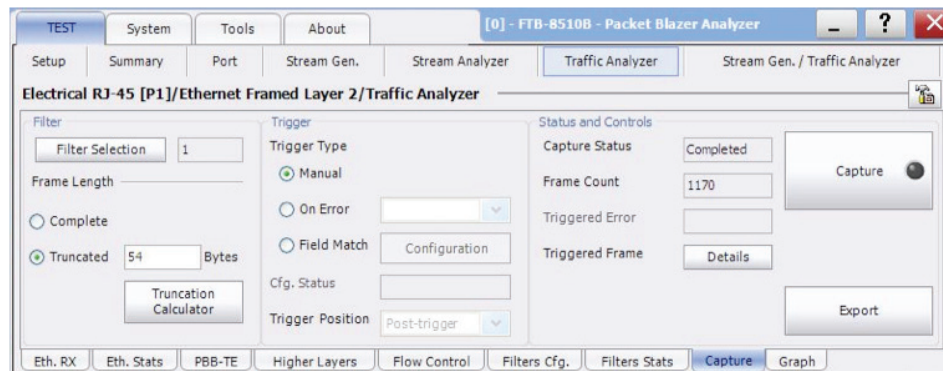
- An example of a PTPv2 packet capture sequence.
- An analysis tool can provide deep-packet decoding and conversation analysis, which can determine issues in the flow of traffic between boundary clocks and grand master clocks.

CURRENT PACKET-CAPTURE ALTERNATIVES

The traditional method for performing packet capture and decoding required extensive hardware and lab equipment to handle the large amount of data and the high packet-rate. As processing power increased, desktops and laptops became viable platforms for simple capture and decode—with dedicated hardware remaining the ideal tools for lab and process-intensive applications. However, as desktop and laptops simplified and made capturing more affordable, along came a number of drawbacks:

- › Using laptops also increases the amount of equipment that a technician must bring to a job site. As technicians become more mobile, controlling the quantity of equipment that is moved from site to site becomes an issue.
- › In an effort to control costs and operating expenses, network operators have reduced testing and troubleshooting budgets to minimum levels, this is why having a dedicated computer for capture and decode functions becomes more and more difficult to justify.
- › Computers and laptops do not usually provide gigabit-rate capabilities and costly adapters, switches or optical/electrical converters must be associated to the capturing device when testing must be performed over gigabit rates or optical connections. Adding these devices increases the complexity of the test architecture and adds extra points-of-failure—something that should be avoided when performing troubleshooting with limited information.
- › As 10GigE links are becoming more popular, engineers are now starting to troubleshoot aggregation points that use 10GigE links. With a typical computer or laptop scenario, 10GigE capabilities are very costly adapters and are usually performed by using a converting switch.

EXFO'S PACKET-CAPTURE AND DECODE CAPABILITIES



In order to enhance troubleshooting tools for technicians and network engineers, EXFO has introduced packet-capture and decode capabilities to its extensive datacom portfolio—as a software upgrade to its existing FTB and RTU Ethernet test modules. This new feature, associated with the frame-analyzer test tool, introduces Ethernet capture capabilities at a line-rate speed from 10 Mbit/s to 10 Gbit/s. The combination of these two tools allows network operators and technicians to quickly and efficiently troubleshoot network events:

- › **Packet capture on a test tool:** By enabling packet capture on the test platform, two of the technician's pains are solved. First, technicians only need to carry one piece of equipment instead of two or more, which provides powerful packet-capture, decode and test capabilities all from one single piece of equipment in the field—therefore reducing equipment costs.
- › **Industry-standard capture files:** Captured traffic is saved in PCAP files, the industry standard in capture data files. Decoding capabilities is performed via Wireshark¹, an industry leader and the de facto standard in packet analysis and decoding. This open-source tool is freely available on the Internet and provides the most complete packet decoding capabilities and powerful post-processing analysis capabilities. Wireshark's strong and committed community of developers ensures that the tool is constantly updated.
- › **Availability on a wide series of modules:** Packet capture is available on almost the entire EXFO datacom portfolio, from the dedicated Ethernet module FTB series to the multiservice PowerBlazer series to the centralized rack-mounted RTU series. The wide availability of form factors and capabilities ensure that solutions can be applied for any network configuration.
- › **Packet capture for all Ethernet rates:** Since packet capture is performed directly from the test ports of the modules, capture can be performed on all Ethernet rates from 10 Mbit/s to 10GigE for LAN and metro networks, and 100GigE for high-speed with full line-rate capabilities. This flexibility removes the need for external accessories and reduces the number of failure points in the test architecture.

¹ Wireshark is available under the GNU General Public License version 2. Wireshark is a trademark of CACE Technologies.

PACKET-CAPTURE USABILITY FEATURES

EXFO's implementation of the packet-capture tool goes beyond the simple capture capabilities. Extra features and functionalities have been implemented in order to increase the efficiency of the test cycle and provide more value to the customer. Capturing capabilities are often reduced by the limited amount of memory available to store the capture traffic. In the case of the EXFO suite, available memory is dependent on the module used. In order to mitigate the effect of these limitations, EXFO's packet-capture tool provides comprehensive filter and triggering methods to target specific traffic and efficiently use the memory available.

Filtering Captured Traffic

In some cases, only a particular traffic flow is of interest and other traffic can consume memory without providing any useful information. The EXFO packet capture tool provides the capability to filter the captured traffic in order to capture only traffic that fits a specific profile, therefore efficiently using the available memory.

The filter engine is based on the basic frame-analyzer and advanced traffic-filter system. In the basic mode, the user can filter traffic based on a single trigger value, while an advanced mode provides the capability to restrict traffic even more by using up to four trigger field and operands (AND, OR, NOT). In both cases, a complete set of triggers is available such as MAC – IP – TCP/UDP fields, VLAN, MPLS and PBB-TE fields.

Packet Truncation

In most captures, the payload information is typically proprietary information that cannot be understood and decoded by the analysis engine. The technical staff usually focuses on header information as these are decoded and are used for more in-depth troubleshooting, such as conversation and top-talker analysis. Therefore, capturing the payload of packets is, in most cases, not efficient as it consumes memory without providing extra information.

EXFO's packet-capture tool provides an innovative packet truncation feature, which limits the capture to a specific number of bytes, starting from the first bit of the packet. Users can therefore limit capture to the first few bytes of the header (layer 2 to layer 4) or add more bytes to include higher layer information. By only capturing this information and avoiding the payload, users efficiently use the available memory. In order to assist the truncation process, a simple calculator is provided. This efficient tool automatically calculates the number of bytes to truncate according to the common header profile of the incoming frames.

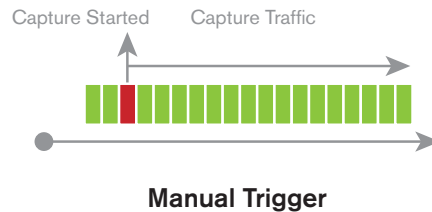
Capture Triggers

A very common issue with typical capture tools is that the capture starts as soon as the tool is enabled. However, the event of interest may occur later and the captured traffic fills the memory buffer but does not provide any useful information. In some cases, the testing opportunity can be completely missed because of the high amount of captured data and the short event window.

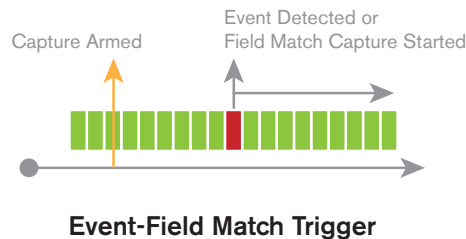
EXFO's packet-capture tools solve this issue by including a set of triggering capabilities, allowing the customer to fine-tune and specify when the capture process should start. This powerful capability simplifies the troubleshooting process by filling the memory only when the event of interest is detected.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

Users can capture traffic based on three types of triggers:

1. 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 and mimics traditional capture tools.



2. On-error trigger is a trigger which 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 can remain armed; monitoring the circuit, until the specific event is detected and the capture is triggered.
3. Field-match trigger launches the capture when a frame with a specific filtered condition is detected. This condition uses a similar system as 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.



Triggering Position

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

A typical use for the triggering position is performing pre- and post-analysis. In network troubleshooting, it is very important to understand the events that lead to the failure and to view the events that followed the failure. These two critical phases provide a wealth of information on the failure, as well as on its causes and how the network reacted to it. For example, troubleshooting a TCP retransmission issue could start by looking at the pre-trigger phase to identify the cause of the retransmission by focusing on the TCP sequence itself, looking at the bandwidth usage or determining if there was any congestion by searching for Ethernet pause frames. The post-trigger analysis can focus on the retransmission process and determine if the cause of congestion has been relieved.

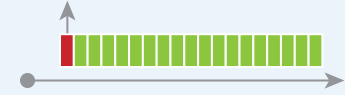
The triggering position capabilities allows the user to specify where the trigger event will be located in the capture, therefore allowing the selection of the frames that will be captured, depending on their position relative to the trigger event. Traditional capture tools do not provide the capability to perform mid-trigger or pre-trigger as they only provide post-trigger capabilities. Instead, users are left to manually search in the captured sequence to identify the event and perform the analysis. Combining this to the lack of trigger mechanism, it is quite possible when using traditional capture tools that the event of interest is completely missed, resulting in an efficient capture process.

EXFO's packet-capture feature provides three triggering positions:

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.

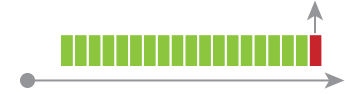
Trigger frame = First frame of the capture



Pre-Trigger

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

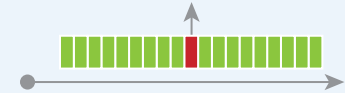
Trigger frame = Last frame of the capture



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.

Trigger frame = Frame in the middle of the capture



EXPORTING CAPTURE AND ANALYSIS

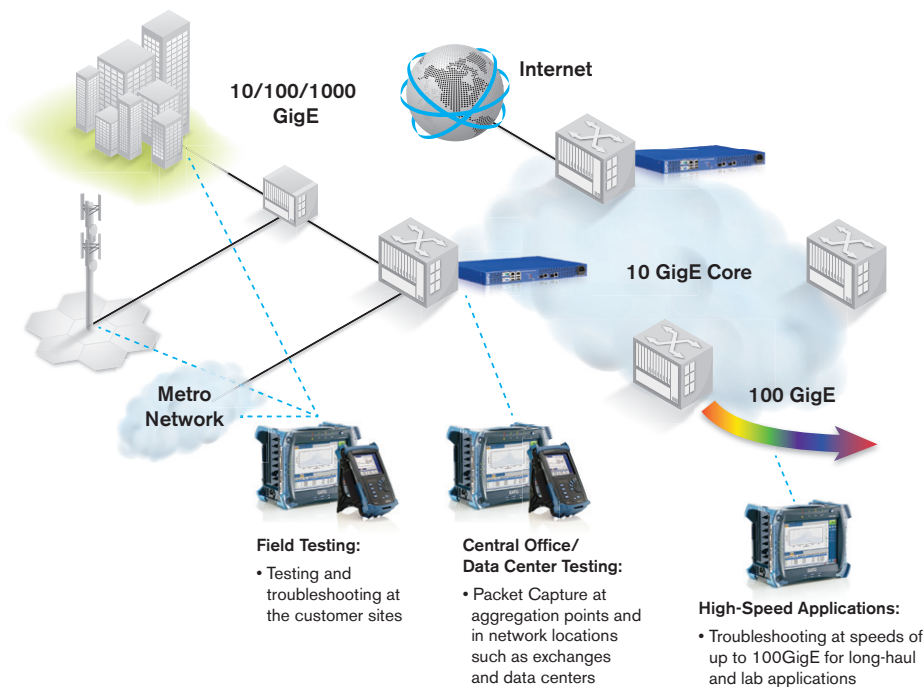
Once a capture has been completed, the captured data can be exported either to the platform's internal memory or to an external USB-based memory for decoding. The exporting process generates an industry-standard, PCAP file that can be used by a variety of open-source decoding tools.

Decoding and post-analysis is performed using the Wireshark application (the industry standard in protocol analysis and decode). This free application enables extensive protocol decoding as well as complex analysis to provide a solid post-processing analysis. Since Wireshark is an open-source application and it is maintained by a strong and dedicated community of developers and contributors, the application is always up-to-date with the latest protocols. What's more, Wireshark is also supported by various extensions that enable analysis tools or specialized processes which can be used to complement the standard Wireshark offering.

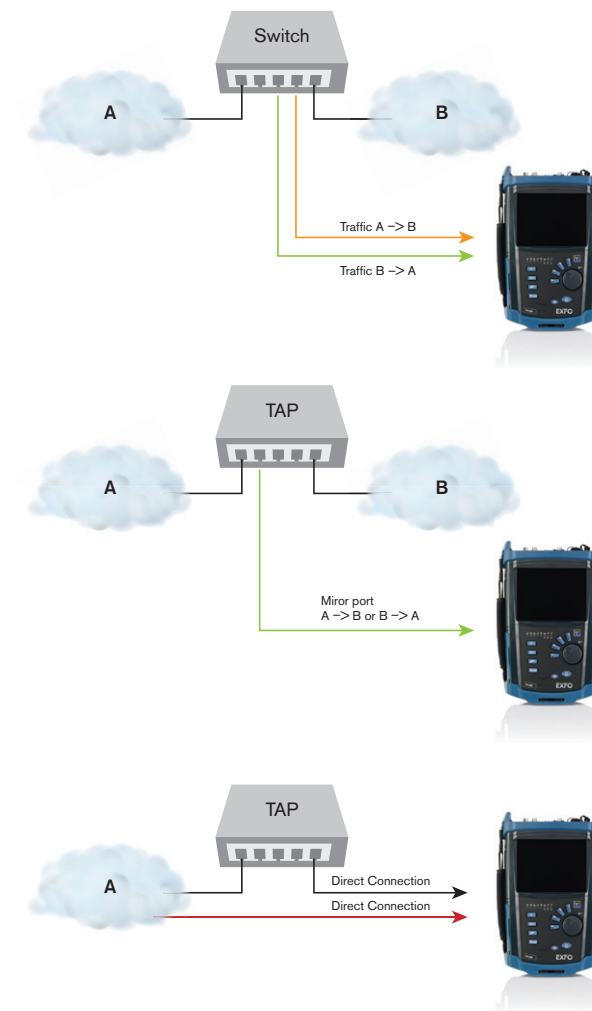
APPLICATION CASE

Testing Locations

EXFO's test solution can be used in a variety of locations, from central field and customer locations to labs and exchange office.



Connection Option



CONCLUSION

Today's multiservice networks are growing increasingly complex, driving the need for technicians to have a more granular view of data traffic across all layers of the network. By adding packet-capture and decode capabilities to its test modules, EXFO brings to market a comprehensive, simplified and fully integrated solution for end-to-end carrier Ethernet network assessment. This enables field technicians to quickly pinpoint, analyze and report quality of service issues using a single test unit. With packet-capture and decode functionalities, EXFO is revolutionizing the way network operators validate, turn up, monitor and troubleshoot carrier Ethernet services.

EXFO Corporate Headquarters > 400 Godin Avenue, Quebec City (Quebec) G1M 2K2 CANADA | Tel.: +1 418 683-0211 | Fax: +1 418 683-2170 | info@EXFO.com

Toll-free: +1 800 663-3936 (USA and Canada) | www.EXFO.com

EXFO America	3701 Plano Parkway, Suite 160	Plano, TX 75075 USA	Tel.: +1 800 663-3936	Fax: +1 972 836-0164
EXFO Asia	151 Chin Swee Road, #03-29 Manhattan House	SINGAPORE 169876	Tel.: +65 6333 8241	Fax: +65 6333 8242
EXFO China	36 North, 3 rd Ring Road East, Dongcheng District Room 1207, Tower C, Global Trade Center	Beijing 100013 P. R. CHINA	Tel.: + 86 10 5825 7755	Fax: +86 10 5825 7722
EXFO Europe	Omega Enterprise Park, Electron Way	Chandlers Ford, Hampshire S053 4SE ENGLAND	Tel.: +44 2380 246810	Fax: +44 2380 246801
EXFO NetHawk	Elektroniikkatie 2	FI-90590 Oulu, FINLAND	Tel.: +358 (0)403 010 300	Fax: +358 (0)8 564 5203
EXFO Service Assurance	270 Billerica Road	Chelmsford, MA 01824 USA	Tel.: +1 978 367-5600	Fax: +1 978 367-5700