138

DETAILED ETHERNET FRAME ANALYSIS WITH EXFO'S EXpertNPA SOFTWARE

APPLICATION NOTE

By Matthew Demyttenaere, Application Engineer

In addition to the usual network tests, service providers need to monitor live traffic to perform higher-layer protocol analyses. This type of testing is important as it can detect the early warning signs of potential problems in the network, or even speed up network troubleshooting without having to disrupt customer traffic. As Ethernet is fast becoming the de facto transmission standard, new tools are required to allow for more detailed analyses of the traffic that is flowing over these networks.

EXFO's latest Ethernet tool – the EXpert Network Protocol Analyzer (NPA) software – was designed specifically for this purpose. Installed on the FTB-400 Universal Test System mainframe, it allows users to carry out higher-layer protocol tests and perform detailed analyses of the frames, as it gives the user the capability to see all the way down to the bytes of the frame. This can be done either out of service, when the traffic is terminated, or using a mirrored port to monitor live traffic.

This application note covers the main applications for this software tool and how it can help network service providers in each of those situations.

Application 1: Locating a source that is broadcasting too much

A network can experience major problems when there are too many broadcasts occurring simultaneously (see Figure 3 in the Appendix below). In fact, the network could slow down significantly because the switches will be forwarding these broadcasts to all switch ports, creating unnecessary traffic. In this type of situation, the EXpertNPA software can be used to monitor the switch(es) and therefore determine which one is causing this excess traffic. To do so, the switch port being monitored must first be configured as a mirrored port, as this allows the user to view live traffic without disrupting it.

With the EXpertNPA software, the user connects the FTB-400 mainframe's PCMCIA port to the mirrored port of the switch and then proceeds to start capturing frames (the number of frames is up to the user). Once this process is complete, one click on the Destination tab will group similar destinations and will display their corresponding sources. By looking at the sources of the Broadcast groups, the user can see if there is a particular source IP address that is continually broadcasting, and thus locate the computer or network device that is causing the problem. Alternatively, one could also view the statistics for the Top Broadcaster List, which displays all the devices broadcasting on the network.

Application 2: Using filters to capture specific protocols

There are instances when frames on specific protocols must be captured; for example, only IP, TCP, UDP, ARP, ICMP, or even a mix of any of these.

IP is a Layer 3 protocol of the OSI reference model and its frames can transport two main types of Layer 4 protocols: TCP and UDP.

The main difference between UDP and TCP is that when TCP frames are sent, an acknowledgement is sent back when the signal arrives at its destination, so the sender (from the TCP perspective) will know whether the frame has been received or not. When UDP frames are sent, however, an acknowledgement is not sent back.

If a user monitors a TCP link between two network devices, he will be able to see the acknowledgements between the two. If any errors occur or if any frames are dropped, TCP retransmission frames will usually appear. If there are many TCP retransmission requests, this could be a sign of problems on the network. One possible problem could be that there is too much line noise, causing the frames to get corrupted somewhere along the way.

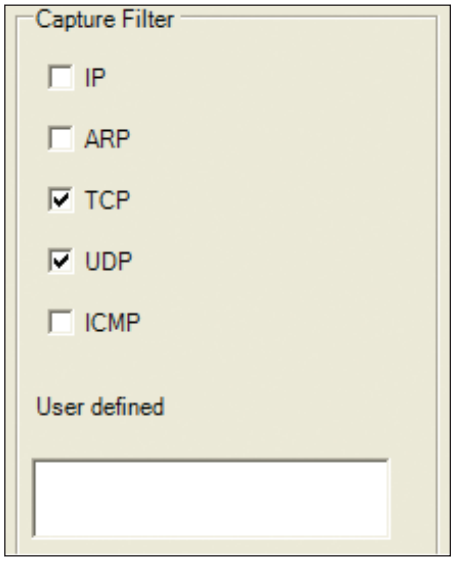

Figure 1

Application 3: Validation of VLAN settings on a switch

There are times when service providers would like to validate that their switches have been configured correctly for VLAN tagging. If the switch has not been configured correctly (e.g., no VLAN tagging has been implemented) then Customer A could potentially have access to sensitive information from Customer B and vice versa (see Figure 4 in the Appendix below). Using the EXpertNPA software, the service provider could capture the frames that are being sent and received on the trunked port and then analyze the VLAN statistics. The statistics provide information such as which VLAN IDs are flowing on this port and what percentage of the port they are using. The utilization becomes important any time there is any traffic-shaping being implemented. This can show the user which VLAN ID is using the most switch port capacity.

Similarly, one can choose different filter types; for example, the user can determine the top broadcasters on the network, or look at the packet-size distribution, etc. Sometimes it is also very useful to look at the conversations that are taking place between different devices on the network. Using the predefined filters can allow a network administrator or a service provider to perform real-time analysis of the network, which can identify potential network problems before they occur.

Used in conjunction with the FTB-8510 Packet Blazer, the EXpertNPA software can be a powerful tool to monitor the health of the network or to troubleshoot, as it can also perform remote testing. The unit can therefore be connected to the remote site that is transmitting frames, allowing users to perform a complete analysis (local and remote) of the frames that are passing through the network.

Figure 2

Appendix

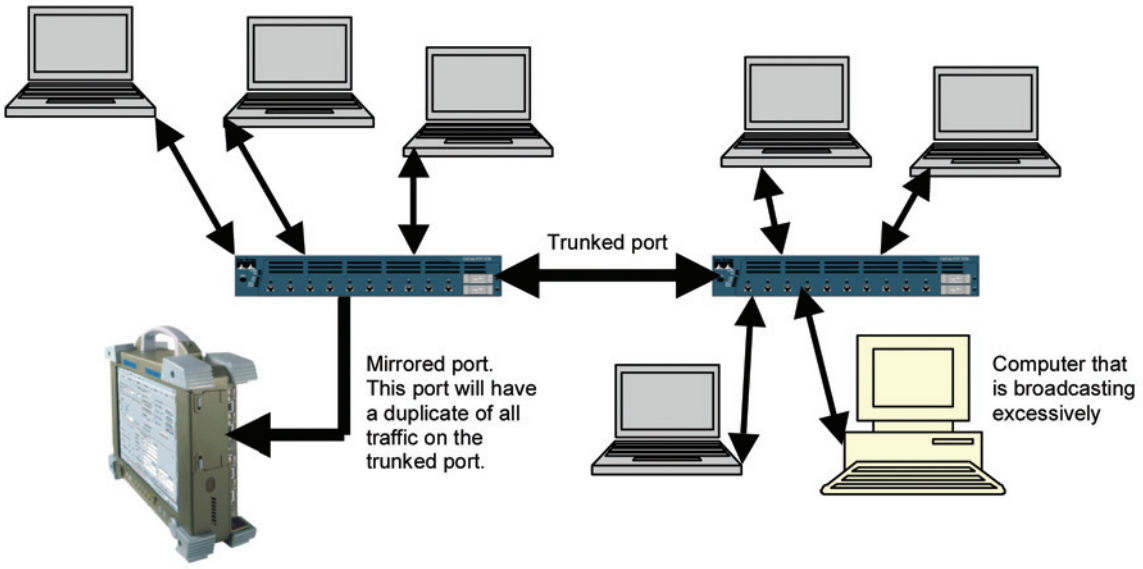

Figure 3

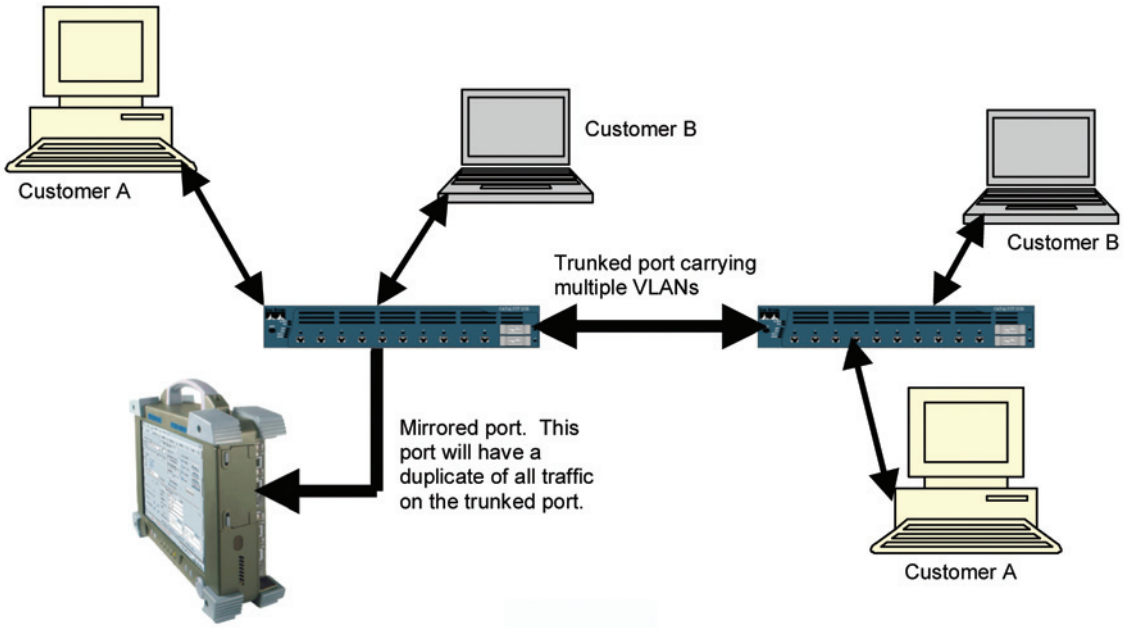

Figure 4

Corporate Headquarters > 400 Godin Avenue, Vanier (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 Park, Suite 160	Plano, TX 75075 USA	Tel.: 1 800 663-3936	Fax: 1 972 836-0164
EXFO Europe	Le Dynasteur, 10/12 rue Andras Beck	92366 Meudon la Forêt Cedex FRANCE	Tel.: +33.1.40.83.85.85	Fax: +33.1.40.83.04.42
EXFO Asia-Pacific	151 Chin Swee Road, #03-29 Manhattan House	SINGAPORE 169876	Tel.: +65 6333 8241	Fax: +65 6333 8242
EXFO China	No.88 Fuhua, First Road Central Tower, Room 801, Futian District	Shenzhen 518048, CHINA	Tel.: +86 (755) 8203 2300	Fax: +86 (755) 8203 2306

Printed in Canada 05/11

EXPERTISE REACHING OUT