

Customer Tips

dc01cc0255
January 15, 2004

... for the user

Network Packet Analyzer Tips

Purpose

This document contains a procedure that Xerox customers can follow to create network traffic captures. Members of Xerox support groups often request a network traffic capture to analyze a device or function failure or to review an example of a working protocol. This document also discusses a popular open-source packet analysis tool that is easy to obtain and use to create packet captures.

Introduction to Packet Capture

Packet capturing refers to the act of recording network traffic and saving this data to a file. The packet capture is later disassembled and its data used to debug a failure. A packet capture session is commonly referred to as a *sniff* or a *trace*, and contains the binary information as seen on the wire from the packet analyzing host's network interface. Specialized software is required to capture this data, special hardware is generally not required (as was common in the past).

Ethereal is an open source network packet and protocol analyzer. Download Ethereal from ethereal.com and follow the instructions to install it on the operating system of your choice.

To obtain a Windows compatible version of Ethereal, download Ethereal and WinCap from the Web sites listed in the "References" section of this document. Run the WinPCap executable to install the library and run the Ethereal setup executable to install that product. Use the defaults for each product's install routine.

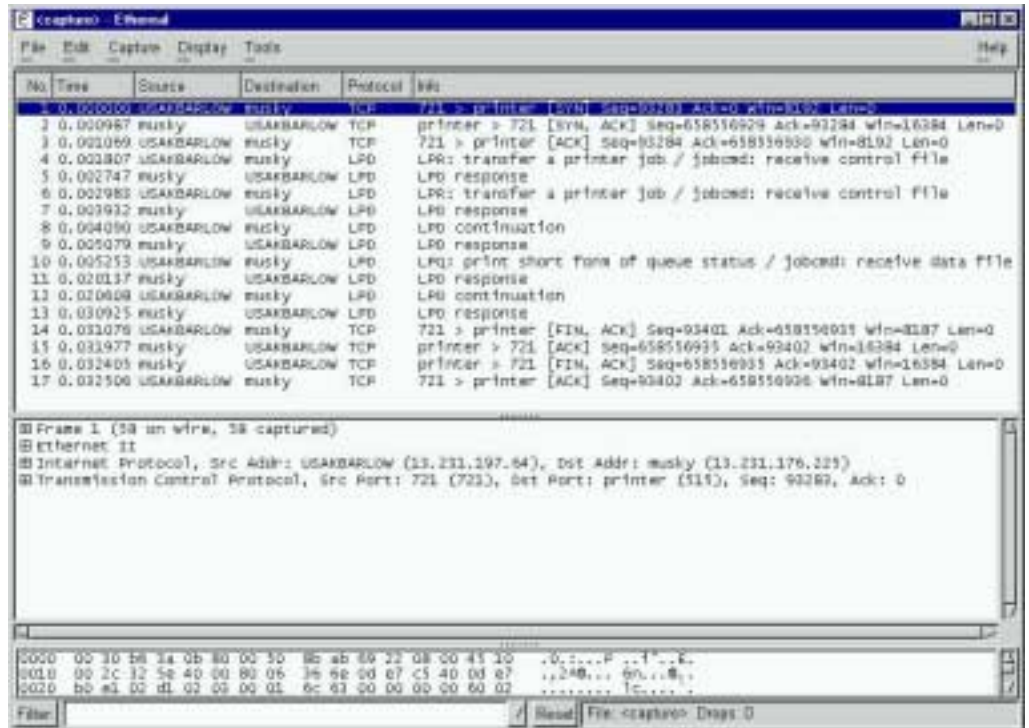
This document applies to these **Xerox** products:

x	WC Pro 32/40 Color
x	WC Pro 65/75/90
x	WC Pro 35/45/55
x	WC M35/M45/M55
x	DC 555/545/535 ST
x	DC 490/480/470/460 ST
x	DC 440/432/425/420 ST
x	DC 340/332 ST
x	DC 265/255/240 ST/LP
x	DC 230/220 ST/LP
x	DCCS 50

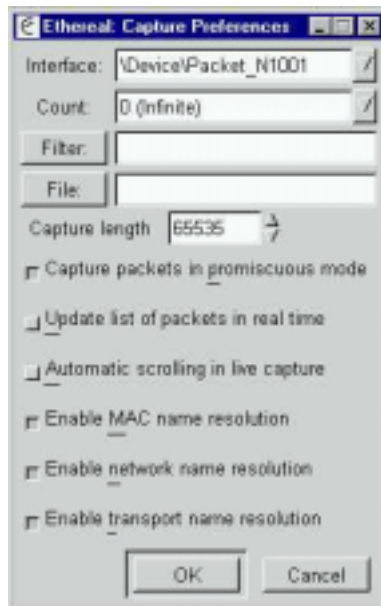
Basic Packet Captures

1. Connect the Xerox multifunction device and the client running Ethereal to the same hub (do not connect the multifunction device and client directly through a switch, see "Connecting Your Packet Analyzer to Your Network," later in this document).
2. After installation, open the Ethereal program.

A main window with a menu bar and three data areas appears. The first data area contains a summary of the packets for analysis, the data area below it contains details of a packet you select, and the third section contains a hexadecimal version of the details.



3. Select **Capture>Start**. The **Capture Preferences** dialog box is displayed.



4. The following choices describe a quick packet capture method and a more generic method:
 - a. Quick Packet Capture (recommended method). In the **Filter** field, enter the word **host**, followed by a **space** and the **ip address** of the printer.
 - b. Generic Packet Capture. Enter a filter name or enable/disable the options in the bottom half of the dialog box to adjust the display filter.

NOTE: For more details about filters, see the "Filter" section later in this document.

5. Click **OK**. The **Capture** dialog box appears. This dialog box counts the packets by protocol.

Protocol	Count	Percentage
Total	259	(100.0%)
SCTP	0	(0.0%)
TCP	80	(30.9%)
UDP	16	(6.2%)
ICMP	0	(0.0%)
OSPF	0	(0.0%)
GRE	0	(0.0%)
NetBIOS	0	(0.0%)
IPX	152	(58.7%)
VINES	1	(0.4%)
Other	10	(3.9%)

Stop

6. Perform the action you wish to have captured. The **Capture** dialog box displays the traffic. Our example shows TCP, UDP and IPX traffic as well as a few packets from the less often used protocols.
7. Click **Stop** to end the capture after the job has printed, or after the amount of time it normally takes to print the job. Ethereal computes the packet analysis and displays it.
8. Save the packet capture file. We prefer that you save the files using the default file type, if a file type change is necessary, save them as **Network Associates Sniffer** (either version).



9. Email the file to Xerox support for further analysis.

Network Packet Analysis Information

Packet capture files are slightly larger than the network traffic they contain. A capture from a session using a 10Mb Power Point presentation print-ready file generates a file larger than 10 Mb.

The following list contains examples of when to create a packet capture:

- A small print file takes an exceedingly long time to start using a particular protocol, but prints immediately using other protocols.
- A user ID on a banner sheet does not match the ID of the user that sent the print job.
- To recreate a print-ready file you cannot acquire through any other means. (Ethereal has a very nice "follow this session" feature, which makes it easy to pull data from streams.)
- A bi-directional driver displays the wrong information about a printer.
- An SMTP mail server fails to work with the scan to SMTP function.

Xerox support is interested in analyzing these items:

- Packets generated during a conversation between two devices, not every packet the network generates during the session.
- The time these events occur: the start of the conversation, the error, and the end of the sniff session.
- The keystrokes or user input that created the session.

Xerox support groups also require the version and name of the program you use to create the packet capture. We use Sniffer Pro, Ethereal, Microsoft's Net Monitor, Network General Packet Analyzer and Sun's command line snoop program delivered with Solaris. We also use the generic Unix based tcpdump program.

Host Information

Record the following relevant host and target information.

- Ethernet addresses included or excluded from the filter and protocols excluded, if any.
- Other identifying information about each host, such as its IP address, to make sorting through the file easier.
- Include configuration sheets for any printers involved.
- Information about a router (if it exists) between host and printer.

This data immediately identifies the devices involved.

Filters

Filters are important to a network trace to eliminate unneeded data and slim down the size of the file. You can use capture filters to limit data during the capture session, and display filters to limit data after the packets are saved. Typically, a filter includes the client, server, and printer in question. In some cases, you include all traffic then use a display filter to view data based on protocol and hosts.

Examples of Filters

Ethereal's filters are based on the libpcap filter language. The following list contains descriptions of Ethereal filters and examples.

- Capture only TCP traffic to and from a particular IP address:
`tcp and host <IP address of target>`
- Capture only LPD traffic from a specific:
`tcp port 515 and host <IP address of target>`
- Capture only port 9100 printing traffic from a host:
`tcp port 9100 and host <IP address of target>`

Ethereal has a graphical filter builder that allows you to choose components from a list. If you need to build a complex filter, use this graphical interface. Use this easy method to create a filter: in **Filter** in the **Ethereal Capture Preference** dialog box, enter "host <IP>" where IP is the IP address of the printer.

Connecting Your Packet Analyzer to Your Network

Place the packet analyzer on the network in the same "collision domain" as the target device. A collision domain is an area on the network capable of seeing **all** packets to and from a particular host. If the target is on a hub, plug your packet analyzer into the same hub. As networks become increasingly switch based, collision domains shrink and performance improves, but require more care to select the right scan source port. Take a packet sample to see if you can watch traffic from the target machine. If you can not see the target, and there are no facilities to attach a hub, ask the network administrator to mirror the switch ports. Mirroring switch ports allows your source machine to scan the target machine as if it were sharing a collision domain.

References

Ethereal is available from <http://www.ethereal.com/> , specifically, the download area for Microsoft Windows NT and other versions of Microsoft Windows is:
<http://www.ethereal.com/distribution/win32/>

The Microsoft Windows version of the Ethereal tool requires an extra file from:
<http://netgroup-serv.polito.it/winpcap>

The download page for WinCap is:
<http://netgroup-serv.polito.it/winpcap/install/default.htm> .

Ethereal's User Guide is available from the Internet:
<http://www.ns.aus.com/ethereal/user-guide/book1.html>

Additional Information

Xerox Customer Service welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA), TTY 1-800-855-2880 or at <http://www.xerox.com>.

Other Tips about Xerox multifunction devices are available at the following URL:
<http://www.xerox.com/DocumentCentreFamily/Tips>.

XEROX®, The Document Company®, the digital X®, and all Xerox product names are trademarks of XEROX CORPORATION. Other trademarks belong to their respective owners.

Copyright © XEROX CORPORATION 2004. All Rights Reserved.

