

How to use a Ethernet Sniffer Program

For some networking applications (i.e. BSD socket programs) it is sometimes necessary to display and analyse the traffic of the Ethernet link between the DIL/NetPC DNP/5280 and other LAN-based systems.

Use a Ethernet LAN sniffer program for this job. The DIL/NetPC DNP/5280 Starter Kit CD-ROM comes with a free (GPL-based) Ethernet LAN sniffer program called *Ethereal*.

- 1. Step (Windows Version): Install *Ethereal* on your Windows-based PC. You find the necessary installation files within the directory \Ethereal-LAN-Sniffer-Win32 of your DIL/NetPC DNP/5280 Starter Kit CD-ROM. Install first the Ethernet packet capture utility *WinPcap 2 3* and then *Ethereal*. Both tools comes within a standard Windows setup file.
- **2. Step**: Run the *Ethereal* LAN sniffer program and capture data. Then display and analyse the data.

	pture> - Eth					
File Edit Capture Display Tools						Help —
No. 🗸	1. The second	Source	Destination		Info	
2 3 6 7 8 9 10 11	0.001298 0.001315 0.011720 1.001957 1.003022 2.003369 2.004415 3.004811 3.005854 5.005017	CPQ19757852914.Belkin 192.168.2.1	CPQ19757852914.Belkin 192.168.2.1 CPQ19757852914.Belkin 192.168.2.1 CPQ19757852914.Belkin 192.168.2.1 CPQ19757852914.Belkin 192.168.2.1 CPQ19757852914.Belkin CPQ19757852914.Belkin	ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	<pre>who has 192.168.2.1? Tell 192.168.2.2 192.168.2.1 is at 00:30:bd:93:c5:38 Echo (ping) request Echo (ping) reply Who has 192.168.2.2? Tell 192.168.2.1 192.168.2.2 is at 00:30:bd:99:50:49</pre>	
<pre> Frame 1 (42 on wire, 42 captured) Arrival Time: Dec 7, 2003 13:48:42.022664000 Time delta from previous packet: 0.000000000 seconds Time relative to first packet: 0.000000000 seconds Frame Number: 1 Packet Length: 42 bytes Capture Length: 42 bytes Ethernet II Destination: ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff</pre>						
⊞ Addi	réss Reso	lution Protocol (reque				
0000 0010 0020	08 00 06	ff ff ff ff <mark>00 30 bd 99</mark> 04 00 01 00 30 bd 99 00 00 00 c0 a8 02 01	9 50 49 08 06 00 01 . 9 50 49 c0 a8 02 02 .		PI PI 	
Filter:	ilter. Apply Source Hardware Address (eth.src), 6 bytes					

That is all.