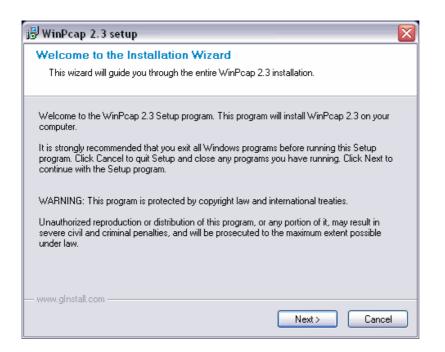


How to use an Ethernet Sniffer Program

The Starter Kit CD-ROM for the DIL/NetPC DNP/9200 comes with a Windows version of the *Ethereal* Ethernet LAN sniffer (the world's most popular network protocol analyzer). Please watch the Internet at <u>http://www.ethereal.com/</u> for newer versions and user documentation.

• **1. Step**: Install the packet capture utility *WinPcap*. Run the executable *WinPcap_2-3* direct from the CD-ROM directory *\Ethereal-LAN-Sniffer-Win32*. Follow the instructions of this install tool.



- **2. Step**: Reboot your Windows PC.
- **3. Step**: Install *Ethereal*. Run the executable *ethereal-setup-0.9.5* direct from the CD-ROM directory *Ethereal-LAN-Sniffer-Win32*. Please follow the instructions of the install tool.

© Ethereal Setup: Installation Directory 🛛 🛛 🔀						
Choose a directory in which to install Ethereal.						
Select the directory to install Ethereal in:						
C:\Programme\Ethereal	Browse					
Space required: 21.1MB Space available: 10.0GB						
Cancel Nullsoft Install System v1.98 < Back	Install					



• **4. Step**: Run *Ethereal* on your PC. First capture Ethernet LAN traffic (menu item *Capture*). Then analyze the results. The following picture shows a sample.

© <capture> - Ethereal</capture>							
File Edit Capture Display Tools Help							
No. 🗸	Time	Source	Destination	Protocol	Info		
	0.000000 3.997722	0.0.0.0	255.255.255.255 255.255.255.255	BOOTP BOOTP	Boot Request from 00:ff:31:d3:39:f0 Boot Request from 00:ff:31:d3:39:f0		
	4.041403 4.080133	192.168.200.40 KDW-NEW-ACER	KDW-NEW-ACER ff:ff:ff:ff:ff:ff	BOOTP ARP	Boot Reply who has 192.168.200.1? Tell 192.168.200.1		
5	5.048822	KDW-NEW-ACER	ff:ff:ff:ff:ff:ff ff:ff:ff:ff:ff:ff	ARP	who has 192.168.200.1? Tell 192.168.200.1		
7	7.078995	KDW-NEW-ACER KDW-NEW-ACER	224.0.0.22	ARP IGMP	who has 192.168.200.1? Tell 192.168.200.1 V3 Membership Report		
		KDW-NEW-ACER KDW-NEW-ACER	192.168.200.255 239.255.255.250	NBNS SSDP	Registration NB KDW-NEW-ACER <00> M-SEARCH * HTTP/1.1		
		KDW-NEW-ACER KDW-NEW-ACER	192.168.200.255 224.0.0.22	NBNS IGMP	Registration NB KDW-NEW-ACER <00> V3 Membership Report		
12	8.634004	KDW-NEW-ACER KDW-NEW-ACER	192.168.200.255 192.168.200.255	NBNS NBNS	Registration NB KDW-NEW-ACER <00> Registration NB KDW-NEW-ACER <00>		
14	10.136774	KDW-NEW-ACER	192.168.200.255	NBNS	Registration NB ARBEITSGRUPPE <00> M-SEARCH * HTTP/1.1		
16	10.887250	KDW-NEW-ACER KDW-NEW-ACER	239.255.255.250 192.168.200.255	SSDP NBNS	Registration NB ARBEITSGRUPPE <00>		
17	11.638322	KDW-NEW-ACER	192.168.200.255	NBNS	Registration NB ARBEITSGRUPPE <00>		
□							
Ethernet II Dinternet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)							
🗄 User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)							
Bootstrap Protocol							
⊠ [0000		ff ff ff 00 ff 3:	 1 d3 39 f0 08 00 45 00				
0010	01 56 00	99 00 00 80 11 3		.V D.C.B	8		
0030	ff 43 00	00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 1 d3 39 f0 00 00 00 00 00				
0050	00 00 00	00 00 00 00 00 0					
0070 0080			0 00 00 00 00 00 00 00 00 0 00 00 00 00		::::::: F		
0090 00a0	00 00 00	00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 0 00 00 00 00				
00b0 00c0	00 00 00	00 00 00 00 00 0	0 00 00 00 00 00 00 00 00				
Filter:				/ Reset A	pply Ethernet (eth)		

Please note: *Ethereal* for Windows needs *WinPcap* for packet capturing. The Internet offers many different versions for *Ethereal* and *WinPCap*. Not every *Ethereal* version works with each *WinPcap* version in your Windows environment. In the case of problems please try different version combinations for *Ethereal* and *WinPcap*.

That's all.