

How to Debug a TCP/IP Communication Problem

- **1. Step**: Download the current evaluation version of Network Spy from *http://network-spy.com*. Network Spy is a *Ethernet Sniffer*. This program allows you to capture and display Ethernet packets. Network Spy also offers a decoder for TCP/IP header and data formats.
- **2. Step**: Install Network Spy on a Windows-based PC. Then set-up a debugging environment. The following picture shows a typical set-up. Don't use a switch in this environment. The two TCP/IP communication partners in this picture are one PC (IP address 192.168.0.1) and one DIL/NetPC (IP address 192.168.0.3).



• **3. Step**: Capture and analyse your TCP/IP communication problems. The debugging strategy is very simple. First capture the TCP/IP traffic between the two TCP/IP communication partners.

	Alerts Counters Arp Table						
	Timestamp Source	Destination	Size	Type	Info	IDS Message	
	09.10.43.610 00.00.39 A8.1C	FF.FF.FF.FF.FF.FF.	60	802.3 frame	type = 0x2200		
	09.10.43.940 192.168.0.3	Broadcast	60	arp req.	192.168.0.1 = ?		
	09:10:44:000 192.168.0.1	192.168.0.3	42	arp resp.	00:40:05:A3:E7:49		
	091044:000 192168.0.3	192.168.0.1	74	icmp	echo request		
woughput:	09.10.44.000 192.168.0.1	192.168.0.3	74	icmp	echo reply		
0.011	09.10.44.980 192.168.0.3	192.168.0.1	74	icmp	echo request		
U.U.Khps	09:10:44:980 192.168.0.1	192.168.0.3	74	icmp	echo reply		
	09 10 45 970 192 168 0.3	192,168.0.1	74	icmp	echo request		
sak Throughout	09.10.45.970 192.168.0.1	192.168.0.3	74	10mp	echo reply		
2.211	09.10.46.960 192.168.0.3	192.168.0.1	74	icmp	echo request		
2.3 KDpc	09:10:47:020 192.168.0.1	192.168.0.3	74	icmp	echo reply		
	091048010 192168.03	192.168.0.1	74	icmp	echo request		
acket Count	09.10.48.010 192.168.0.1	192.168.0.3	74	icmp	echo reply		
1 12	09.10.48.990 192.168.0.3	192.168.0.1	74	icmp	echo request		
21	09.10.48.990 192.168.0.1	192.168.0.3	74	icmp	echo reply		
	09:10:49:980 192:168:0.3	192.168.0.1	74	icmp	echo request		
ytes:	09.10.50.040 192.168.0.1	192.168.0.3	74	10mp	echo reply		
1.848	09.10.51.030 192.168.0.3	192.168.0.1	74	10mp	echo request		
1	09:10.51:030 192.168.0.1	192,168.0.3	74	icmp	echo reply		
	091052010 192168.0.3	192 168 0 1	74	icmp	echo request		
me Elapsed	09.10.52.010 192.168.0.1	192.168.0.3	74	icmp	echo reply		
00:00:42	09/10/53/000 192/168/0/3	192.168.0.1	74	icmp	echo request		
00.00.43	0910.53000 192.168.0.1	192.168.0.3	74	KCMP	echo reply		
	091054:050 192158:0.3	192 168 0 1	74	reub	echo request		
	09.10.54.050 192.168.0.1	192.168.0.3	74	icmp	echo reply		
	091055040 192168.0.3	192.168.0.1	74	KUUD	echo request		
	03:10:55:040 192.168.0.1	192.168.0.3	/4	icmp	echo reply		



• **4. Step**: Analyse the TCP/IP packets. Each packet in the capture buffer is one line within the Network Spy main window. A simple mouse click to a line opens a decoder window.

🛃 Decoder									
<u>File</u> <u>P</u> acket									
ee K									
Packet Timestamp: 9:10:48:010 🛛 💦 着									
Ethernet_II Frame Header									
Source Address:	00:00:39:A8:1C:B2								
Destination Address:	00:40:05:A3:E7:49								
Туре:	0x0800								
·									
IP Header									
Version:	4								
Length:	5 (20 bytes)								
Type of Service:	0×00								
Precedence	Routine								
Minimize Delay	0								
Maximize Throughput	0								
Maximize Reliability	0								
Minimize Monetary cost	0								
Total Length:	60 bytes								
Identification:	5888								
Flags:	0×0								
Don't fragment:	0								
More fragments:	0								
Fragment Offset:	0								
Time-to-live:	32								
Protocol:	UXU1 (ICMP)								
Checksum:									
Dest IP Address:	192.100.0.3								
	172.100.0.1	•							
	00 00 30 10 00 00 00 45 00								
	00 39 A8 10 B2 08 00 45 00 01 02 6D C0 A8 00 03 C0 A8	< m							
0020 00 01 08 00 36 50 02	00 15 00 61 62 63 64 65 66	6\abcdef							
0030 67 68 69 6A 6B 6C 6D	6E 6F 70 71 72 73 74 75 76	ghijklmnopqrstuv 🦰							
0040 77 61 62 63 64 65 66	67 68 69	wabcdefghi							