EasyTrace LAN Analysis

The **EasyTrace LAN Analysis Software** is an optional part of the main *EasyTrace for Windows* software package. It expands your personal computer into a powerful network diagnostic tool with the approved EasyTrace desktop. Outside the software *EasyTrace for Windows* and a packet driver which is part of the software package you only need one or several network interface cards. All established NICs are supported. An optional seperate TAP dongle for non–invasive network analysis is available.

The packet driver activates the network interface card(s) in the *Promiscuous Mode*, so all packets are captured by the EasyTrace application software. The packets will be fitted with time stamps and will be saved into files on the hard disk. The EasyTrace desktop shows all data in a protocols view in a decoded and clearly readable form. So network analysis is supported online and offline.

Every network interface card which is designated for LAN analysis has to be connected to a point of interest for analysis, normally by a patch cable (RJ 45). Analysis ports may be link ports or mirror ports (SPAN ports, switch or hub). Alternatively you can use the output ports of a TAP dongle which supports capturing of data of a certain link in a read-only mode without any influence to the link.

EasyTrace can write every packet to the hard disk or certain packets only, limited by filtering functions. You can capture your data without limitations in time or EasyTrace can generate files in intervals and at certain dates (*File Split*).

Supported Protocols:
802.2, 802.3, 802.1Q, 802.1p, PPPoE/PPPoA (T-DSL), X.25, X.75 over Ethernet, IPX, Cisco-HDLC, MLP (PPP) Multilink, PPP (all control protocols), PAP, CHAP, BAP, LCP, SNAP, ARP, RARP, OSPF, IPv4, ICMP, RSVP, IGMP, DHCP, BOOTP, TCP, UDP, RTCP, RTP, H.323, NetBIOS, DNS, SNMP*, SIP*, SMB, T.38 (FoIP- Fax over IP), ISIS, Kerberos, compression protocols: LZS Stack (PPP), MPPC Microsoft (PPP),

Extensive Analysis Options:
- Lists of TCP sessions, PPP connections and IP packets
- Analysis of data throughput, packet flow (graphically), protocol statistics and protocol errors
- RTP analysis
- Import and export of data in several file formats

It is an interesting option that you can manage capture sessions with several PCs at several points of measurement at the same time. The time stamps of packets in EasyTrace are synchronous to the system clock of MS Windows. If the system clocks of all EasyTrace computers are synchronized by an NTP client, all packets in EasyTrace files are synchronized too.

- Follow the process of TCP sessions and let you show the workload of TCP ports. You will get interpretations of delays in your network in relation to the request for ports caused by certain services.
- Watch the way and the runtime of IP packets exactly on the basis of the packet ID. You can measure the average delay of IP packets between measurement points and IP addresses. So you will get statements about conspicuous delay of received packets and routing problems in your network.
- EasyTrace helps to detect delays resulting from network utilization and network configuration problems. Helpful statistics will give you an overview about the common efficiency in your network.

Summary

Scope of Delivery:
- CD ROM incl. application software and NDIS driver to enable LAN trace function for the PC NIC. Optional: TAP dongle incl. driver software
- Printed manual.

System Requirements:
PC (Desktop or Notebook) with Intel or AMD CPU (min. 2.4 GHz) and min. 2 GByte RAM.

Microsoft Windows XP / Vista / W7, W8 (32bit)

Supported Protocols:
802.2, 802.3, 802.1Q, 802.1p, PPPoE/PPPoA (T-DSL), X.25, X.75 over Ethernet, IPX, Cisco-HDLC, MLP (PPP) Multilink, PPP (all control protocols), PAP, CHAP, BAP, LCP, SNAP, ARP, RARP, OSPF, IPv4, ICMP, RSVP, IGMP, DHCP, BOOTP, TCP, UDP, RTCP, RTP, H.323, NetBIOS, DNS, SNMP, SIP, SMB, T,38, ISIS, Kerberos, compression protocols: LZS Stack (PPP), MPPC Microsoft (PPP) and many others.
New protocols and filters are added continuously

Please contact us for individual enhancements of implemented protocols.

Decoding and Capturing:
- Fully automatic protocol detecting and decoding for implemented protocols.
- Decoding display wide configurable.
- Remote access to start and configure capturing
- Continuous capturing and file splitting for unlimited time.
- Configurable live trigger sends alerts via email.*

Saving data, opening of saved files and printing data:
- Saving, opening and printing of captured data automatically or manually.
- Filing of continuous data streams daily, weekly or in intervals at free selectable points in time incl. automatically creation of several reports and analyses.
- Saving data with user-defined file information.
- Automatically creation of project files which integrate all involved files of a capture session in a project.

Filtering Data:
- Filter for Ethernet, IP, PPP, TCP, UDP, HEX-Bytes, packet length.
- Filtering of protocols, addresses, frame types, IP options, port numbers, fragments, directions.
- Filters can be configured as capture filter or display filter.
- All filters can be saved in a list of filter profiles (portable to another PC/Notebook).
- Combination of single filters in Boolean equations.
- All activated filters are arranged and displayed in a hierarchical tree structure.
- Alternation between filtered data views inside the tree structure.

Flexible functions for searching time stamps or frames and text elements in the decoded data view.

Overviews and Analyses:
IP Packets: Time stamps, IP address of source and destination, packet ID, TTL, protocol.
TCP Sessions:
Time stamps, IP address of source and destination incl. port numbers, period of a session, transmitted and received amount of data, repetitions.
PPP connections:
Time stamps, direction, trials of connections, endpoint ID, login, transport, compression, block size, transmitted amount of data, protocols.
Media connection:
LAN SIP or H.323, Time stamps, direction, transport, compression,

Analyses and statistical functions (excerpt)
- **Data Throughput**
- **Active Lines / active sessions over time**
- **Protocol usage statistics**
- **Top-Talkers (on protocol level)**
- **Top-Users (on session level)**
- **Station activity**
- **RTP Jitter/Delay estimation**
- **Protocol and Link errors**
- **Many more…**

All statistics are versatile configurable. Data can be related to subsets off all data. Filters may be automatically generated from the statistic data to relate to protocol events.

Supported File Formats:
Sniffer, Acterna Examine, LibPcap, LibPcapNG transparent binary format, Wireshark

Optional Hardware Component**:
TAP for undisturbed trace of a link available on request.
- USB 3.0 interface
- Displayed as an NIC in EasyTrace interface selection
- Fast Ethernet (100 MBit/s & 1G)
- Power supply via USB

In Progress:
- Scalable measurement system, remote handling (SSL encrypted)
- Displaying of assignment between MAC address and IP address.
- Database connectivity to store results in MySQL
- Native 64-bit support

* Coming soon
** Optional equipment