EasyTrace LAN Software

Die **EasyTrace LAN** Software ist ein optionales Modul aus unserem Softwarepaket *EasyTrace für Windows*. Unter der bewährten Oberfläche machen Sie Ihren PC zu einem leistungsfähigen Netzwerkdiagnose-Werkzeug. Neben der Software *EasyTrace für Windows* und einem Paket-Treiber, der im Lieferumfang enthalten ist, benötigen Sie nur noch eine oder mehrere Ethernet-Netzwerkkarten. Alle gängigen Karten werden unterstützt. Optional ist ein TAP zur nichtinvasiven Überwachung eines Links verfügbar.

Der Paket-Treiber versetzt die Ethernet-Karte(n) in den *Promiscuous Mode*, in dem alle Pakete an die EasyTrace-Applikation geleitet werden. Die Pakete erhalten Zeitstempel und werden in Dateien auf der Festplatte gespeichert. Gleichzeitig erfolgt die Anzeige der Daten in der EasyTrace-Protokolle-Ansicht. Somit ist die Analyse eines Netzwerksegments online oder offline möglich.

Jede zur Analyse bestimmte Netzwerkkarte des Analyse-PC wird mit einem Patch-Kabel mit einem Analysepunkt verbunden. Als Analysepunkte kommen Link-Ports oder Spiegel-Ports (SPAN-Ports) an Switches (eine Netzwerkkarte im Analyse-PC) in Frage, oder der Ausgang eines TAP zum passiven Abgriff der Daten eines Links.

Bei der Aufzeichnung der Daten können Sie alle erfassten Datenpakete abspeichern oder Sie beschränken die Aufzeichnung durch Filteroptionen auf bestimmte Details. Zusätzlich haben Sie die Wahl, dauerhaft aufzuzeichnen oder vollautomatisch Dateien in Intervallen oder zu bestimmten Zeiten erzeugen zu lassen.

Folgende Protokolle werden unterstützt:
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 (alle Control-Protokolle), PAP, CHAP, BAP, LCP, SNAP, ARP, RARP, OSPF, IPv4,IPv6, ICMP, RSVP, IGMP, DHCP, BOOTP, TCP, UDP, RTCP, RTP**, H.323**, NetBIOS, DNS, SNMP*, SIP**, Compression Protokolle: LZS Stack (PPP), MPPC Microsoft (PPP), FoIP T.38/ T.30/ T.4**, Radius Diameter Protokoll

Umfangreiche Auswertungsmöglichkeiten stehen in EasyTrace LAN zur Verfügung:
- Listen von TCP-Sitzungen, PPP-Verbindungen und IP-Paketen
- Analyse des Datendurchsatzes, des Paketflusses (grafisch), Protokollstatistiken und Protokollfehler
- RTP-Analyse
- Import und Export von Daten in verschiedenen Formaten
- Alarmierung bei Verhaltensmustern*

Es können mit einem oder mit mehreren PCs Messungen an mehreren Analysepunkten gleichzeitig vorgenommen werden. Im Falle von mehreren PCs lassen sich synchrone Zeitstempel erzielen, da sich *EasyTrace für Windows* bei der Ermittlung der Zeitstempel mit der Uhr des PC synchronisiert und die PC-Uhren untereinander durch Abgleich z. Bsp. mit einem NTP-Server synchronisiert werden können.

- Verfolgen Sie den Verlauf von TCP-Sitzungen und lassen Sie sich anzeigen, welche Ports wie oft und wie lange beansprucht wurden. Erhalten Sie anschauliche Darstellungen von Verzögerungen im Netz, die bei erhöhter Nachfrage nach bestimmten Diensten an bestimmten Ports auftreten.
- Beobachten Sie den Weg und die Laufzeit von IP-Paketen gezielt anhand der Packet-ID. Messen Sie die durchschnittliche Laufzeit der IP-Pakete zwischen bestimmten Messpunkten und zu bestimmten IP-Adressen. Erhalten Sie Aussagen zu auffälligen Verzögerungen beim Empfang von IP-Paketen und Routing-Problemen in Ihrer Infrastruktur.
- Erkennen Sie Verzögerungen an den von EasyTrace überwachten Netzwerkknoten und extrahieren Sie schnell die wesentlichen Informationen über die allgemeine Netzwerkauslastung.

HERAKOM GmbH
Wolfsbachweg 62, 45133 Essen, Tel. 0201 / 46694223, Fax: 0201 / 46694232, E-Mail: Heikeh@Herakom.de, http://www.herakom.de
HRB Essen 11 694, Steuernummer: 112/5960/0479, Ust.-Id-Nr.: DE 811945307, Geschäftsführerin: Heike Hüttemann
Bankverbindung: Sparkasse Essen Haarzopf, BLZ 360 501 05, Kto. Nr. 3 303 393

Die Technik in Stichworten

Lieferumfang:
CD-ROM mit Applikationssoftware und NDIS-Treiber für LAN-Trace über die PC-Netzwerkkarte, unterstützt wird der Spiegelport (automatische Duplikatserkennung), Deutsche Dokumentationen. Optional: TAP inkl. Treiber

Hardwarevoraussetzungen:
PC/Notebook mit Intel-/AMD-CPU ab 1 GHz und min. 256 MByte RAM (min. 512 MByte für Windows XP SP2), Lauffähig in einer virtuellen Umgebung (ähnlich wie bei der virtuellen VLAN Technik)

Softwarevoraussetzungen:
Microsoft Windows 2000 (SP4) oder XP (SP2), Windows 7/8, VM Ware

Unterstützte Protokolle:
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 (alle Control-Protokolle), PAP, CHAP, BAP, LCP, SNAP, ARP, RARP, OSPF, IPv4, IPv6, ICMP, RSVP, IGMP, DHCP, BOOTP, TCP, UDP, RTCP, RTP, H.323**, NetBIOS, DNS, SNMP*, SIP**, Compression Protokolle: LZS Stack (PPP), MPPC Microsoft(PPP) FoIP T.38/ T.30/ T.4, Diameter Radius** u.v.m.

Dekodieren und Aufzeichnen:
- Automatische Protokollerkennung und Dekodierung der enthaltenen Protokolle
- Online Defragmentierung v. Protokollen (selektiv abschaltbar
- Monitoring mit mehreren Schnittstellen mit Scroll-Synchronisation bei mehreren Aufzeichnungs- fenstern
- Konfigurierbare Duplikatserkennung für Traces am Spiegelport (Mirrorport)
- Umfang der Anzeige konfigurierbar

Speichern, Laden und Drucken:
- Speichern, Laden und Drucken von aufgezeichneten Daten automatisch im Hintergrund oder manuell.
- Ablage gesplitteter Dateien täglich, wöchentlich oder in Intervallen zu frei wählbaren Zeitpunkten inkl. automatischer Erstellung verschiedener Auswertungen und Übersichten.
- Speicherung von Dateien mit benutzerdefinierten Datei-Informationen.
- Automatische Erstellung von Projektdateien mit Zusammenfassung aller Dateien einer Arbeitssitzung.
- Auswertung und Grafiken als PDF, PNG, BMP usw. oder über die Zwischenablage möglich.

Filtern der Daten:
- Filter für Ethernet, IP, PPP, TCP, UDP, HEX-Bytes, Paketlänge.
- Filterung nach Protokollen, Adressen, Rahmentypen, IP-Optionen, Port-Nummern, Fragmente, Richtungen
- Filter wirken wahlweise als Aufzeichnungs- oder Anzeigefilter
- Alle Filter in einer Liste als Filterprofil speicherbar (Liste kann auf andere PCs übertragen werden).
- Logische Verknüpfungen einzelner Filterkriterien.
- Anzeige der aktiven ausgewählten Filterprofile in einer Baumstruktur
- Wechsel zwischen den gefilterten Ansichten innerhalb des Filterbaums
- Verhaltensfilter*

Weitere Eigenschaften der Filter
Alle Filter in einer Liste als Filterprofil speicherbar, Anwendung als Aufzeichnungs oder Anzeigefilter, Logische Verknüpfungen einzelner Filterkriterien. Anzeige der aktiven ausgewählten Filterprofile

Flexible Suchfunktion nach Zeit oder Frame und Textsuche in den dekodierten Daten

Framezähler

Übersichten:
IP-Pakete: Zeitstempel, Quell- u. Ziel-IP-Adresse, Packet-ID, TTL, Protokoll
TCP-Sitzungen:
Zeitstempel, Quell- und Ziel-IP-Adresse inkl. Portnummern, Dauer, gesendete und empfangene Datenmenge, Wiederholungen
PPP-Verbindungen:
Zeitstempel, Richtung, Versuche, Endpunkt-ID, Login, Transport, Komprimierung, Blockgröße, gesendete Datenmenge, Protokolle

Auswertungen/Statistikfunktionen
Datendurchsatz:
Grafische und numerische Anzeige der Datenrate, getrennt für Rx-/Tx-Richtung. Darstellung absolut oder prozentual, Werte dezimal oder mit binärer Basis, Auflösung von 1 Sekunde bis 1 Stunde pro Messintervall
Grafische Paketflussanalyse:
Die Auslastung der o. g. Funktionen wird in Grafik- und Tabellenanzeigen dargestellt.
Protokollstatistik:
Es wird eine tabellarische und Grafische Übersicht über Summenzähler in Paketen, Bruttovolumen, Nutzlastvolumen und Fehlern für jede dargestellte Strukturschicht angezeigt. Eine schichtenorientierte Farbgebung der Tabelle wird unterstützt. Grafiken sind speicher- und druckbar.
Protokollfehler:
Grafische Auswertung aller erkannten Protokollfehler, Fehler im TCP-Protokoll.
RTP-Analyse:
Jittermessung für VoIP (SIP**, H.323**)
Top Talker Statistik:
In Tabellen und/oder Grafischer Darstellung wählbar fallend/ steigend. Umfangreiche Filtermöglichkeiten. Grafiken sind speicher- und druckbar u.v.m.

Unterstützte Formate:
Sniffer, Acterna Examine, Ethereal (LibPcap), Wireshark, transparentes Binärformat.

Dateien können im csv Format gespeichert werden

Optionale Hardware-Ausstattung:
TAP** zur nichtinvasiven Überwachung eines Links.
- Anschluss an den PC über USB 2.0 und/oder USB 3.0
- Erscheint als Netzwerkkarte in der Schnittstellen-Auswahl von EasyTrace
- Verfügbar bis Gigabit- Ethernet (10/100/1000MBit/s in Kürze 10Gigabit*)
- Stromversorgung über USB (nur bei dem Modell bis 100Mbit´s); sonst mit Netzteil

Automatische Steuerung über Kommandozeilen-Befehle (Command Line Interface, CLI)**

TLS- Entschlüsselung**
Verschlüsselte Rufe (SRTP) können entschlüsselt werden (sofern Schlüssel und Passwort bekannt sind).

Alarmierung bei Verhaltensmustern*+**
„EasyTrace Script- Sprache- Modul. Das Modul bietet z.B. die Möglichkeit bei einer Daueraufzeichnung des Netzverkehr´s viele Bedingungen zu hinterlegen um Alarme auszulösen. Folgende Themen können mit dem Erweiterungmodul abgesichert werden: Ereignisse, Manipulationen, Angriffe usw.

In Vorbereitung:
- Web-Interface**: - aktuelle Snapshots ausgewählter Ansichten (Statistiken) können über eine Webschnittstelle, mit erweiterten Funktionsumfang auch per Smartphone, für definierbare Anwender zugänglich gemacht werden. (Auf Grund von Limitierungen des Übertragungsnetzes kann hier grundsätzlich keine Live-Funktion angeboten werden.
- SkalierbaresMesssystem,Remotebedienung(SSL-verschlüsselt(*)(**)

Die mit *gekennzeichneten Funktionen sind in Kürze verfügbar und mit ** gekennzeichneten Funktionen sind optional verfügbar.

HERAKOM GmbH
Wolfsbachweg 62, 45133 Essen, Tel. 0201 / 46694223, Fax: 0201 / 46694224, E-mail: Heike@herakom.de, http://www.herakom.de
HRB Essen 11 694, Steuernummer: 112/5960/0479, Ust.-Id-Nr.: DE 811945307, Geschäftsführerin: Heike Hüttemann
Bankverbindung: Sparkasse Essen Haarzopf, BLZ 360 501 05, Kto. Nr. 3 303 393