

COMPROTware:Testtool

COMPROTware:Testtool

Einführung und Schulung

Real Thoughts GmbH

Haid-und-Neu-Straße 7

76131 Karlsruhe

Germany

Fon +49-721-6276730, Fax +49-721-6276731

Website www.realthoughts.de

E-Mail info@realthoughts.de

Das vorliegende Material ist urheberrechtlich geschützt. **Kein Teil darf ohne schriftliche Genehmigung von Real Thoughts** in irgendeiner Form durch Fotokopie, Microfilm oder anderen Verfahren **reproduziert oder** in eine für Maschinen, insbesondere Datenverarbeitungsanlagen, verwendbare Sprache **übertragen werden**. Auch die Rechte der Wiedergabe durch Vortrag, Funk und Fernsehen sind vorbehalten. Ebenso ist **die Weitergabe an Dritte ohne ausdrückliche schriftliche Genehmigung von Real Thoughts streng untersagt**.

COMPROTware:Testtool Allgemein

Allgemein

- **CPTT** ist ein Integriertes Testtool für fernwirktechnische Übertragungsprotokolle
- ... vereint verschiedene Protokolle unter einer Bedienoberfläche
- ... simuliert entweder Master oder Slave Station eines fernwirktechnischen Systems
- ... hört die Kommunikation auf der seriellen Leitung oder im Netzwerk mit

```

COMPROTware:Testtool - Hongkong - File: L:\... \dnp3_001.mlg
File Edit Operate Extra Help
11:11:33.963
  Used protocol profile: "DNP3-1999: Source Addr.: 1, Destination Addr.: 1"
  Used timeout intervals: "Message T0=1s, Link Down T0=7s"
  Serial device "COM5" opened: 9600 baud, 8 data bits, no parity and 1 stop bits, 3ms gap supervision time
11:11:33.963
  Test for Slave ...
11:11:34.976
  Station B->A Link established
11:11:35.017
  Station A->B Link established
11:11:37.070  1 -> 1
  Read #0
  Class 0 Data (Static Data): All objects
11:11:37.124  1 -> 1  Confirm #0
11:11:37.290  1 -> 1
  Response #0 [IIN: ClassAv DvceRestr]
  Binary Input: 14..+16..29
    Bit 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
  ( 14+ 0) 0x5001|off ON off ON off off off off off off off off off off ON
  Binary Input: 33..+16..48
    Bit 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
  ( 33+ 0) 0x0000|off off off off off off off off off off off off off off off
  Binary Output Status: 0..+4..3
  ( 0+ 0) 0x01|off local remote comlst restrt ONLINE
  ( 0+ 1) 0x01|off local remote comlst restrt ONLINE
  
```

Auslieferung

- Zum Lieferumfang gehört
 - ▲ Gedruckte Installationsbeschreibung
 - ▲ CD-ROM mit Installation, Dokumentation und Beispielen
 - ▲ USB-/Parallel Port-/PCMCIA-Dongle zur Lizenzierung der Protokolle

COMPROTware:Testtool CD-ROM & Doku

CD-ROM

- CD-ROM enthält die Installation, die Dokumentation und die Beispiele.

Dokumentation

- Das Verzeichnis `\doc` enthält die Beschreibung zur Software selbst: Installationsanleitung, Benutzerhandbuch und Programmer's Guide; Alles steht in Deutsch und in Englisch bereit, das Benutzerhandbuch zusätzlich in Italienisch
- In `\doc\Support` sind Beschreibungen zu Problemen mit **CPTT** oder zu weitergehenden Themen wie Lizenzupdate enthalten
- In `\doc\Marketing` ist das Datenblatt, die Endanwenderpreisliste und die Präsentation gespeichert

COMPROTware:Testtool Installation

Installation CPTT

- Die Installation von **CPTT** selbst basiert auf Microsoft Windows Installer
- Sie ist in der Installationsanleitung umfangreich beschrieben
- Neue Releases werden parallel zu alten installiert; Bei möglichen Problemen mit neuer Release hat man noch Zugriff auf alte Release; Alte Releases können über Microsoft Windows Installer sehr schnell deinstalliert werden
- Installation erfolgt in fünf Schritten (Reihenfolge beliebig; Dongle **nicht** notwendig):
 - ▲ Installation Java Runtime Environment für Windows x86 (32 Bit):
<http://java.com/download>
 - ▲ Installation WibuKey Runtime für Windows (Windows 32/64 Bit, mehrsprachig):
<http://www.wibu.com/de/anwendersoftware.html>
 - ▲ Installation **COMPROTware:Testtool**
Start über \iX86_WIN32\CPTT\setup.exe
 - ▲ Installation WinPcap
<http://www.winpcap.org/>
 - ▲ Installation **RIO Server**
Die Installation dieser Option ist im zugehörigen Abschnitt weiter unten beschrieben.
- Normalerweise können immer die Standardwerte verwendet werden

COMPROTware:Testtool Lizenzierung

Lizenzierung

- Zur Simulation und zum Mithören ist eine Lizenz (ein aufgesteckter Dongle) notwendig; Off-line Analyse kann jederzeit auch ohne Dongle erfolgen
- **CPTT** darf beliebig auf allen Rechner installiert werden; Nur zur Simulation und zum Mithören ist eine Lizenz notwendig
- Auf dem Dongle sind die protokollspezifischen Lizenzen gespeichert; Nur wenn Lizenz für das Protokoll vorhanden ist, dann kann simuliert/mitgehört werden
- Die Dongles sind beliebig programmierbar:
 - ▲ Über ein Bitmuster auf dem Dongle wird festgelegt, welche Protokolle lizenziert sind
 - ▲ Pro Protokoll kann nur eine Lizenz gespeichert werden; Aber für alle Protokolle kann eine Lizenz gespeichert sein
 - ▲ Über Remote Programming kann durch Austausch einer Kontext-Datei und einer Update-Datei die Programmierung eines Dongles auch über elektronische Medien erfolgen
- Die Dongles sind lieferbar als
 - ▲ Dongle für USB-Anschluß
 - ▲ Dongle für Parallel Port-Anschluß
 - ▲ Dongle für PCMCIA-Anschluß
 - ▲ Für weitere Informationen zu den Dongles siehe auch <http://www.wibu.de/>

COMPROTware:Testtool

Start und Allgemeines

Start

- Wie unter MS Windows üblich kann **CPTT** über das Start-Menü oder das Icon auf dem Desktop gestartet werden
- Zum Start wird die Schlusskonfiguration der letzten Programmausführung wiederhergestellt.
- **CPTT** kann beliebig oft auf einem Rechner gestartet werden und auch mehrere Simulationen gleichzeitig durchführen
- Auch **User Engine Classes** (siehe weiter unten) können zum Programmstart eingelesen und gestartet werden

Allgemeines zum Umgang

- Der Umgang mit **CPTT** entspricht den unter MS Windows üblichen Regeln; Durch Shortcut Keys können häufig gebrauchte Funktionen schnell erreicht werden
- Die folgenden Dateierweiterungen sind mit **CPTT** assoziiert:
 - ▲ .mlg für Message Log-Dateien (Mitschrift des Protokollverkehrs)
 - ▲ .mls für Message List-Dateien (Nachrichtenlisten)
 - ▲ .cptt für Konfigurationsdateien (Parametersätze)
- **CPTT** unterscheidet vier Betriebsmodi:
 - ▲ Reine Darstellung von Protokollverkehr (*Action -> Stop*)
 - ▲ Simulation eines Masters (*Action -> Simulate Master*)
 - ▲ Simulation eines Slaves (*Action -> Simulate Slave*)
 - ▲ Mithören (*Action -> Monitor*)

COMPROTware:Testtool Beispiele

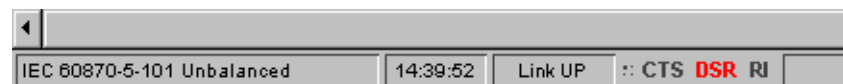
Beispiele

- Die mitgelieferte Beispiele für Nachrichtenlisten unter `c:\Programme\realthoughts\comprotware\testtool\doc\<RELEASE>\MLS_Examples` mit dem Namensbestandteil `*_Std_Example.mls` realisieren immer eine vollständige Demo von Master und Slave;
Die Nachrichtenlisten müssen unter *Edit -> Message List Storage ...* über den Menüpunkt *File->Open from ...* eingelesen werden
- Je nachdem, welches Protokoll Sie lizenziert haben:
 - ▲ Ist es ein serielles Protokoll? Dann verbinden Sie einfach zwei serielle Schnittstellen Ihres Computers miteinander und lassen Sie über die eine Schnittstelle die Master-, über die andere Schnittstelle die Slave-Simulation laufen
 - ▲ Noch einfacher wird's bei netzwerkbasierter Protokollen: Einmal simuliert das laufende Programm die Slave, das andere mal die Master Station (dazu muss als IP-Adresse jedesmal 127.0.0.1 (Localhost) angegeben werden)
- Die mitgelieferten Beispiele sollen helfen **CPTT** zu verstehen und einen Einblick in die Protokolle zu geben

COMPROTware:Testtool Simulation

Simulation

- **CPTT** kann für alle realisierten Übertragungsprotokolle sowohl Master als auch Slave (bzw. Controlling und Controlled Station bzw. Master und Outstation) simulieren
- Zuerst über *Edit -> Protocol Profile ...* das gewünschte Protokoll aus einer Protokollfamilie auswählen; Der Stationsname dient zur leichteren Zuordnung der Fenster zueinander
- Im nächsten Fenster müssen die protokollspezifischen Parameter angegeben werden; Für jedes Protokoll existiert ein eigener Satz Parameter und eine eigene Eingabemaske; Die Standardeinstellung von **CPTT** entspricht üblichen Anwendungsbedingungen
- Jetzt kann über *Action -> Simulate Controlling Station/Action -> Simulate Master* oder *Action -> Simulate Controlled Station/Action -> Simulate Slave* entweder Leit-system oder Unterstation simuliert werden; Durch *Action -> Stop* wird die Simulation wieder gestoppt
- In der Titelzeile des Fenster wird der Operationsmode dargestellt: Controlling, Master, Controlled, Slave, Monitor, ...
- In der Fusszeile wird das ausgewählte Protokoll, die aktuelle Uhrzeit, den Zustand der Verbindung (UP, down), der Empfang von Zeichen mittels Animation und die Modemsignale CTS, DSR und RI dargestellt:



COMPROTware:Testtool
Simulation

Simulation - Fortsetzung

- Die Zuordnung des Nachrichtenverkehrs geschieht über Farben:
 - Die Umrandungsfarbe des Darstellungsfensters gibt den Operationsmodus an
 - Von **CPTT** gesendete Nachrichten sind fett gedruckt
 - Bei IEC 60870-5-104: **Grün** immer Controlling, **Blau** ist immer Controlled
 - Bei seriellen Protokollen: **Grün** immer Master, **Blau** ist immer Slave;
Außer bei IEC 60870-5-101 balanced: **Grün** immer dir, **Blau** ist immer DIR

```
COMPROTware:Testtool - Karlsruhe - Controlling
File Edit Operate Extra Help

Used protocol profile: "IEC 60870-5-101: Transm.proc.: unbalanced, Link Addr.: 1, C
Used timeout intervals: "Message T0=1s, Link Down T0=7s"
Serial device "COM2" opened: 9600 baud, 8 data bits, no parity and 1 stop bits, 100
18:25:10.293
Test for Controlled Station ...
18:25:10.450
Link established
18:25:10.538 M_EI_MA_1 [init +] 1 0 COI=local power switch on, initializat
18:25:10.574 C_IC_MA_1 [act +] 1 0 QOI=Station interrogation (global)
18:25:10.730 C_IC_MA_1 [actcon +] 1 0 QOI=Station interrogation (global)
18:25:10.806 M_SP_MA_1 [inrogen +] 1 1 SPI=1|0n [IV nt sb bl]
18:25:10.870 M_DP_MA_1 [inrogen +] 1 2 DPI=0|Int [IV nt sb BL]
18:25:10.926 M_DP_MA_1 [inrogen +] 1 10203 DPI=1|0ff [IV nt sb BL]
18:25:10.994 M_DP_MA_1 [inrogen +] 1 10204 DPI=2|0n [IV nt sb BL]
18:25:11.072 M_DP_MA_1 [inrogen +] 1 10205 DPI=3|Ind [IV nt sb BL]
18:25:11.123 M_SP_TB_1 [inrogen +] 1 10101 SPI=1|0n [IV MT sb bl] 99
18:25:11.203 M_SP_TB_1 [inrogen +] 1 10102 SPI=0|0ff [IV MT sb bl] 99

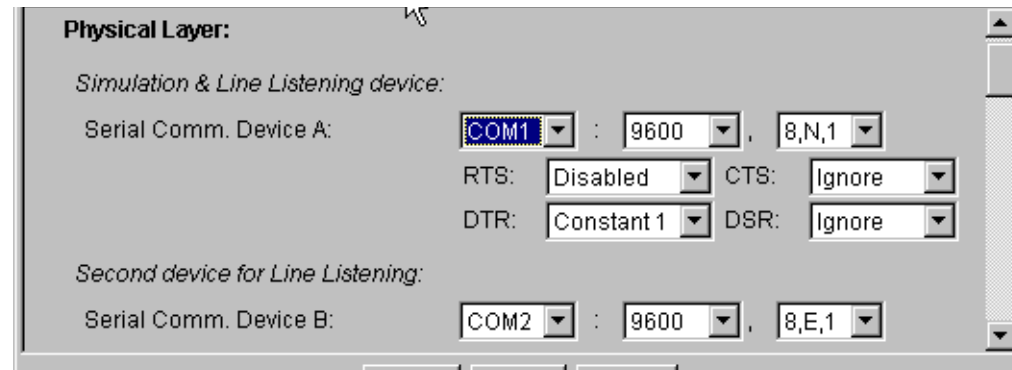
IEC 60870-5-101 Unbalanced 18:25:21 Link UP :: CTS DSR RI
```

- Zum Zustand der Verbindung (dargestellt in der Fusszeile) ist zu sagen:
 - Link down: Es ist keine Verbindung etabliert; Bei Simulation Master versucht **CPTT** durch Verbindungsneustarttelegramme die Verbindung aufzubauen
 - Link UP: Eine Verbindung etabliert; Nachrichten auf der Anwendungsschicht können ausgetauscht werden

COMPROTware:Testtool Protokollprofile

Protokollprofile

- Physikalische Schicht bei seriellen Protokollen:



- ▲ Über Serial Comm. Device A läuft die Simulation ab;
Die hier dargestellte Einstellung für die Modemsignale entspricht einer Direkten Verbindung
- ▲ Serial Comm. Device B und Serial Comm. Device A werden für das Mithören bei seriellen Protokollen gebraucht; Die Modemeinstellungen wird dann ignoriert


COMPROTware:Testtool
Protokollprofile

Protokollprofile - Fortsetzung

- Physikalische Schicht bei netzwerk-basierten Protokollen:


Physical Layer:

According to standard:

Controlled Station IP Address:  127 . 0 . 0 . 1

Port No.: 2404

Implementation specific:

Controlling Station IP Address:  127 . 0 . 0 . 1

Network Adapter (for Listening): [2] SiS 900 PCI Fast Ethernet Adapter

- ▲ Controlled Station IP Address gibt bei der Simulation einer Controlling Station die IP Adresse des Controlled Station an; 2404 ist die Portnr. für den Verbindungsaufbau entsprechend der IEC 60870-5-104-Norm
- ▲ Beim Mithören sind die Controlled Station IP Address und die Controlling Station IP Address Filter für die Darstellung von Netzwerkpaketen; Der Wert 255 ist dabei der Wildcard Value

COMPROTware:Testtool
Protokollprofile

Protokollprofile - Fortsetzung

- Verbindungsschicht, Angaben entsprechend dem Standard:

LPCI:

According to standard:

Transmission Procedure: unbalanced

Direction Bit: 1

Address length [octets]: Link: 1

Link Address: 1

Struct. Link Address Format: %d Decimal

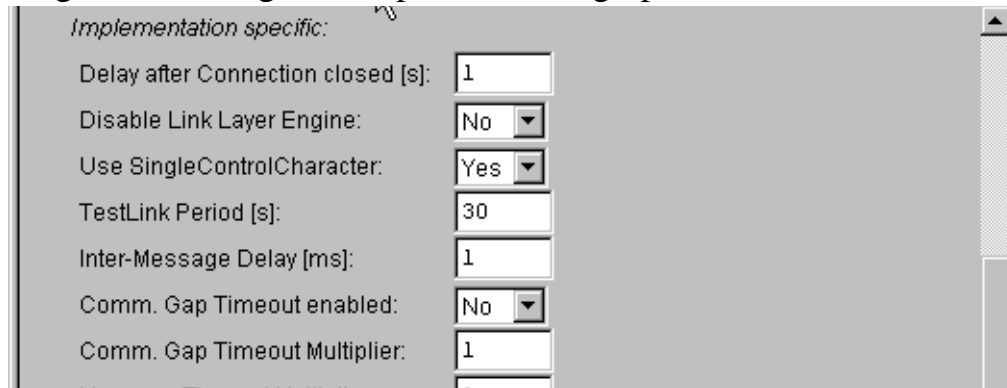
Frame length (net) [octets]: 255

- ▲ Transmission Procedure: unbalanced (unsymmetrisch, Aufrufbetrieb) oder balanced (symmetrisch, spontan)

COMPROTware:Testtool
Protokollprofile

Protokollprofile - Fortsetzung

- Verbindungsschicht, Angaben implementierungsspezifisch:



- ▲ Delay after Connection closed: Verzögerungszeit nach Verbindungsverlust, bevor ein Neuaufbau der Verbindung versucht wird
- ▲ Disable Link Layer Engine: Zustandsmaschine der Verbindungsschicht ist deaktiviert (z.B. für Verbindungsaufbau)
- ▲ Use SingleControlCharacter: Soll das Einzelzeichen 0xe5 verwendet werden?
- ▲ TestLink Period: Periodendauer für TestLink-Zyklus
- ▲ Inter-message Delay: Min. Wartezeit zwischen der zuletzt empfangenen und der nächsten zu schickenden Nachricht
- ▲ Communication Gaps sind Übertragungslücken zwischen zwei Zeichen; Innerhalb eines Telegramms darf es keine davon geben; Hier kann die Überwachung auf Übertragungslücken eingeschaltet und der Timeout für tolerierte Lücken vervielfacht werden

COMPROTware:Testtool Protokollprofile

Protokollprofile - Fortsetzung

- Verbindungsschicht, Angaben implementierungsspezifisch:

The screenshot shows a configuration window with the following settings:

Message Timeout Multiplier:	1
Link Down Timeout Multiplier:	1
Test&Act - 2x-, 1xACD:	No
Test&Act - 2x-, 1xDFC:	No

- ▲ Message Timeout Multiplier: Multiplikator für die Wartezeit, innerhalb der eine Nachricht eingetroffen sein muss; Basiszeit wird anhand der Nachrichtenlänge und der Baudrate berechnet
- ▲ Link Down Timeout Multiplier: Multiplikator für die Wartezeit, bei deren Überschreitung ein Verbindungsverlust erkannt wird; Basiszeit wird anhand der Nachrichtenlänge und der Baudrate berechnet
- ▲ Test&Act - 2x-, 1xACD: Falls gesetzt wird bei der Controlled-Simulation bei jeder dritten Antwort das ACD-Bit gesetzt
- ▲ Test&Act - 2x-, 1xDFC: Falls gesetzt wird bei der Controlled-Simulation bei jeder dritten Antwort das DFC-Bit gesetzt

COMPROTware:Testtool
Protokollprofile

Protokollprofile - Fortsetzung

- Anwendungsschicht, entsprechend dem Standard und implementierungsspezifisch:

ASDU:

According to standard:

Address length [octets]: Common: 1 Inform.Obj.: 2

Field length [octets]: Cause of Transm.: 1

Struct. Common Address Format: %d Decimal

Struct. Info. Obj. Address Format: %d Decimal

Implementation specific:

Auto ACTCON&ACTTERM: Yes

- ▲ Auto ACTCON&ACTTERM: Falls gesetzt, dann wird auf Befehle automatisch ein ACTCON und ggf. ein ACTTERM gesendet

COMPROTware:Testtool Simulationsbeispiele

Simulationbeispiele

- Jetzt sollte das Beispiel für IEC 60870-5-101 bzw. -104 eingelesen werden; Dazu die Dateien `IEC60870_5_101n104_Std_Example.mls` und `IEC60870_5_101n104_All_TypeIdents.mls` einlesen (beim Einlesen der letzten Datei den Message List Storage nicht löschen)
- **CPTT** kann mehrfach auf einem Rechner laufen: Benutzen Sie Ihren Rechner gleichzeitig als Master und Slave; Netzwerk-basierte Protokolle können Sie über die IP-Adresse 127.0.0.1 (Localhost) simulieren, für serielle Protokolle müssen Sie die beiden seriellen Schnittstellen über ein Kabel miteinander verbinden

COMPROTware:Testtool Navigation

Navigation

- Über *Cursor hoch* und *runter*, über *Bild hoch* und *runter* und *Pos1*, *STRG+Pos1* und *Ende* kann im Darstellungsfenster navigiert werden
- Normalerweise ist die Darstellung bei der neuesten Nachricht eingerastet, sodass der aktuelle Protokollverkehr fortlaufend dargestellt wird
- Durch Hochblättern wird die Rastung gelöst, die Darstellung bleibt stehen; Man kann in der feststehenden Darstellung navigieren
- Zur aktualisierenden Darstellung kehrt man durch Drücken von *Ende* zurück
- Auch während der Simulation und des Mithörens kann beliebig im Speicher navigiert werden

COMPROTware:Testtool Darstellungsmodi

Darstellungsmodi

- Das Fenster mit den Darstellungsmodi erscheint über das Hintergrundmenü (rechte Maustaste) und *Formatting Options ...*; Gleichzeitig kann über die Shortcut Keys , <v>, <h> und <l> der Darstellungsmodus gewechselt werden
- Darstellungsmodi (beliebig kombinierbar):
 - ▲ Nur Uhrzeit oder auch mit Datum
 - ▲ Umfassend, mehrzeilig

```
09:45:28.465
9|M_ME_NA_1|measured value, normalized value
VSQ [SQ, N=7], [COT=20|inrogen, tst pn], Originator=0x00
CA=4351
IOA=131124
NVA=0x110b|0.133148
QDS [iv nt sb bl ov]
```

oder prägnant, einzeilig

```
09:45:28.465 M_ME_NA_1 [inrogen +] 4351 131124 NVA=0.133 [iv nt sb bl ov]
( 131124+1 ) NVA=0.298 [iv nt sb bl ov]
( 131124+2 ) NVA=-0.421 [iv nt sb bl ov]
( 131124+3 ) NVA=0.260 [iv nt sb bl ov]
```

- ▲ Inklusive Hexdump

```
09:45:28.465
0x68 0x22 0x18 0x00 0x02 0x00 0x09 0x87 0x14 0x00
0xff 0x10 0x34 0x00 0x02 0x0b 0x11 0x00 0x17 0x26
0x00 0x2b 0xca 0x00 0x57 0x21 0x00 0xc0 0xe4 0x00
0xeb 0xd5 0x00 0xd7 0x21 0x00
M_ME_NA_1 [inrogen +] 4351 131124 NVA=0.133 [iv nt sb bl ov]
( 131124+1 ) NVA=0.298 [iv nt sb bl ov]
```

- ▲ Mit oder ohne Link Layer

```
09:45:28.465
I: SSN=12, RSN=1
M_ME_NA_1 [inrogen +] 4351 131124 NVA=0.133 [iv nt sb bl ov]
( 131124+1 ) NVA=0.298 [iv nt sb bl ov]
( 131124+2 ) NVA=-0.421 [iv nt sb bl ov]
( 131124+3 ) NVA=0.260 [iv nt sb bl ov]
( 131124+4 ) NVA=-0.213 [iv nt sb bl ov]
```

COMPROTware:Testtool
Darstellungsmodi

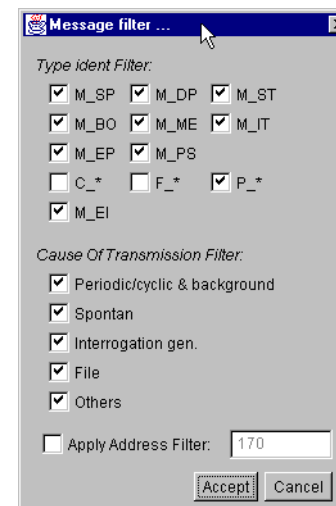
Darstellungsmodi - Fortsetzung

- Speziell für auf dem Netzwerk mitgehörte Informationen (und nicht bei Simulation): Darstellung des Ethernet Frames und/oder des TCP Headers möglich

```
00-09-22 09:45:28.465
Ethernet frame:
 00:10:7B:7F:FC:07 <- 00:00:23:09:01:27; Type=0x0800
IP datagram:
  Vrsn=4, HdrLen=5*32bit, ToS=0, Length=184; Id=1120, Flgs=0, FrgmOfst=0; Ttl=64, Prtcl=6, Chksm=2723
 172.28.144.3 -> 172.28.131.1
TCP header:
 Port: 2404 -> 3494
 SeqNo=2404421902, AckNo=1037098064
 Data Offset=5*32bit, Control Bits=0x18|urg ACK PSH rst syn fin, Window=8192; Cksm=53765, UrgntData=0

      M_ME_NA_l [inrogen +] 4351 131124 NVA=0.133 [iv nt sb bl ov]
                          ( 131124+l ) NVA=0.298 [iv nt sb bl ov]
```

- Filter für Typkennungen, Übertragungsursachen und Stationsadresse über *Formatting Options ... -> Message Filter ...*



COMPROTware:Testtool
Darstellungsmodi

Darstellungsmodi - Fortsetzung

- Der Darstellungsmodus kann jederzeit auch während der Simulation oder des Mithörens geändert werden
- Durch eine graue Wellenlinie wird angezeigt, dass an dieser Stelle Nachrichten herausgefiltert (nicht dargestellt) wurden

```

09:45:28.465 M_ME_NA_1 [inrogen +] 4351 131153 NVA=0.105 [iv nt sb bl ov]
( 131153+1 ) NVA=0.294 [iv nt sb bl ov]
( 131153+2 ) NVA=0.209 [iv nt sb bl ov]
( 131153+3 ) NVA=0.189 [iv nt sb bl ov]
( 131153+4 ) NVA=0.000 [iv nt sb bl ov]
~~~~~
09:45:32.211 M_ME_NA_1 [inrogen +] 4351 131159 NVA=0.248 [iv nt sb bl ov]
( 131159+1 ) NVA=0.000 [iv nt sb bl ov]
( 131159+2 ) NVA=0.000 [iv nt sb bl ov]

```

COMPROTware:Testtool Darstellung Infoelemente

Darstellung Informationselemente

- Übergreifende Regeln zur Darstellung:

```
09:45:28.465
  9|M_ME_NA_1|measured value, normalized value
    VSQ [SQ, N=7], [COT=20|inrogen, tst pn], Originator=0x00
    CA=4351
      IOA=131124
        NVA=0x110b|0.133148
          QDS [iv nt sb bl ov]
```

- ▲ Alternative Darstellungen (z.B. dezimal und Klartext) werden durch | getrennt; Hilfreich, da oft Codierung und Klartext oder Dezimal- und Hexwert von Interesse sind
 - ▲ Gruppierungen sind durch [und] umklammert und meist benannt; So lässt sich die Verbindung zur Hexdarstellung leicht ermitteln
 - ▲ Alle Bits werden dargestellt, gesetzte in Gross- sonst in Kleinbuchstaben; Man weiss immer, welche Kennungen ein Elemente hat
- Bei Darstellungsmode BRIEF werden nur einzelne Darstellungsformen verwendet, bei VERBOSE werden alle notwendigen ausgegeben

COMPROTware:Testtool IEC - Strukturierte Adressen

IEC 60870-5-101/-104 - Strukturierte Adressen

- Strukturierte Adressen teilen die Adresse-Oktette in kleinere Einheiten auf
- **CPTT** bietet eine sehr flexible Darstellung:
 - ▲ Bitgruppen können benannt werden
 - ▲ Darstellung in dezimal und hexadezimal
 - ▲ Vorbereitete Muster erleichtern die Auswahl
- Aufbau: V=%23_16d Fld=%15_8d Grt=%7_0d ist 8-8-8
 - ▲ Zeichenkette kann beliebige Zeichen enthalten
 - ▲ % (Fluchtsymbol) leitet einen Wert ein, %% ergibt %
 - ▲ Optional: Bitpositionen werden vom höchsten zum niedrigsten Bit angegeben; obere Bitposition wird durch _ von unterer getrennt
 - ▲ Für dezimale Darstellung folgt nun d, für hexadezimale x
 - ▲ Werden keine Bitpositionen angegeben, dann wird das gesamte Adressfeld verwendet
 - ▲ %23_16d gibt an, dass die Bits 23 bis 16 (beginnend mit Bit 0) dezimal ausgegeben werden sollen
 - ▲ %d|%x bedeutet, dass das Adressfeld zuerst in dezimal und dann in hexadezimal ausgegeben wird, getrennt durch ein |, also z.B. wie 192|0xc0

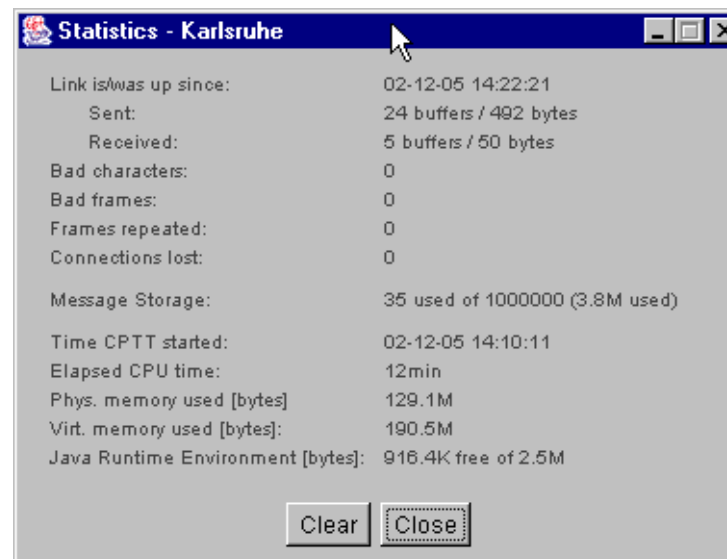
COMPROTware:Testtool Einstellungen & Statistik

Einstellungen

- Zur Kontrolle des Speicherverbrauchs kann die Größe des Message Storage (Speicher für den Protokollverkehr) auf einen Wert zwischen 3.000 und 1.000.000 begrenzt werden (*Edit -> General Preferences ...*)
- Reine Link Layer-Informationen können direkt verworfen werden (*Edit -> General Preferences ...*). Damit verschwendet das Event Polling keine Einträge im Message Storage

Statistik

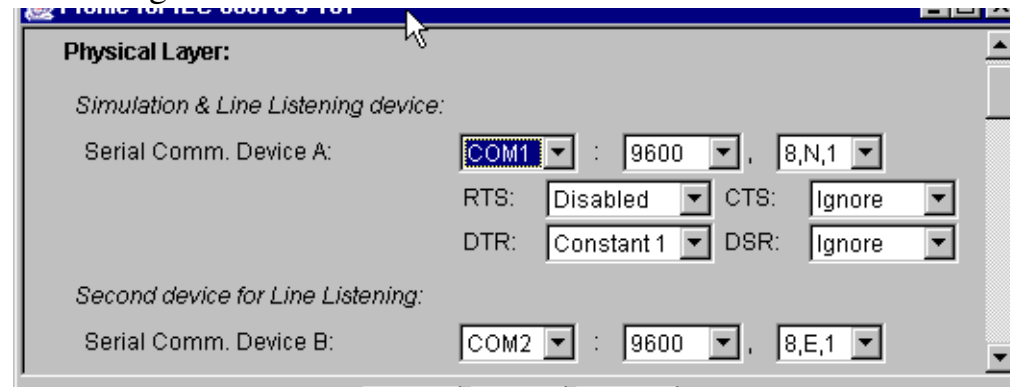
- Verschiedene statistische Größen zur laufenden/letzten Verbindung und zu **CPTT** zeigt das Fenster *Extra -> Statistics* an; Die Größen werden zyklisch aufgefrischt



COMPROTware:Testtool Mithören

Mithören

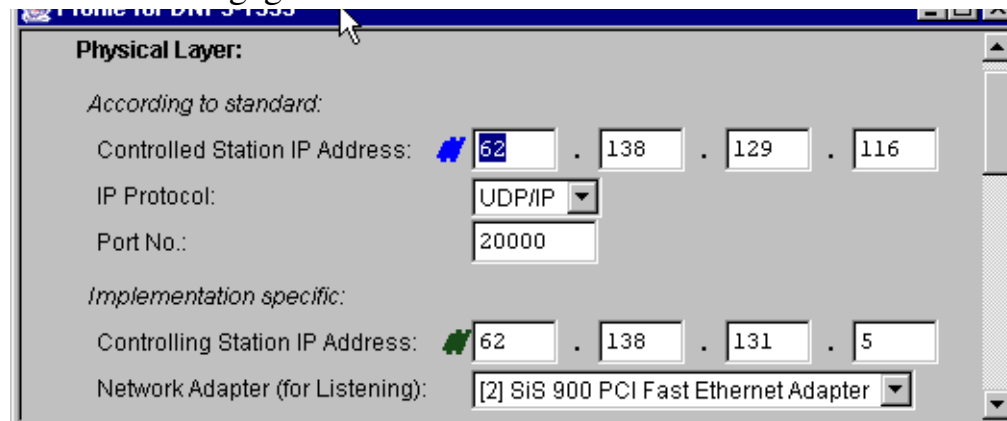
- Mithören ist bei seriellen Protokollen mit zwei seriellen Schnittstellen und bei netzwerk-basierten Protokollen über die Netzwerkkarte möglich
- Besonderheiten beim Mithören netzwerk-basierter Protokolle: Unter MS Windows sind keine weiteren Komponenten notwendig, ein besseres Ergebnis wird aber durch Installation von WinPcap erreicht; Mithören von IEC 61850 GOOSE nur mit WinPcap möglich
- Mithören wird über *Action -> Monitor* gestartet und durch Auswahl von *Action -> Stop* wieder gestoppt
- Bei seriellen Protokollen: Die beide serielle Schnittstellen zum Mithören werden im Protokollprofil aus der Liste der verfügbaren Schnittstellen ausgewählt; Die Modem-signale werden ignoriert:



COMPROTware:Testtool
Mithören

Mithören - Fortsetzung

- Bei netzwerk-basierten Protokollen: Für das Mithören auf dem Netz muss im Protokollprofil die IP Adresse beider Teilnehmer und der Netzwerkkarte angegeben werden; Falls eine IP Adresse veränderlich ist (Redundante Netzwerkkarten), kann 255 als Wildcard Value angegeben werden:



- ▲ Nur bei DNP3 over LAN/WAN: Auswahl des Übertragungsprotokolls: UDP/IP oder TCP/IP
- ▲ Network Adapter gibt die Netzwerkkarte an, die auf dem Netz lauscht
- ▲ Es kann nur der Netzwerkverkehr mithört werden, der an der Netzwerkkarte vorbei verläuft
- ▲ Switches dienen der Optimierung der Netzlast, Hubs nur der Verteilung des Netzwerkverkehrs; Ein Switch leitet Netzwerkpakete nur den Empfänger weiter und verhindert damit, dass man den Netzwerkverkehr mithören kann

COMPROTware:Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- Genormte Modelle für den Informationsaustausch:

ISO/OSI Referenzmodell

Application Layer	7
Presentation Layer	6
Session Layer	5
Transport Layer	4
Network Layer	3
Link Layer	2
Physical Layer	1

Internet Protocol

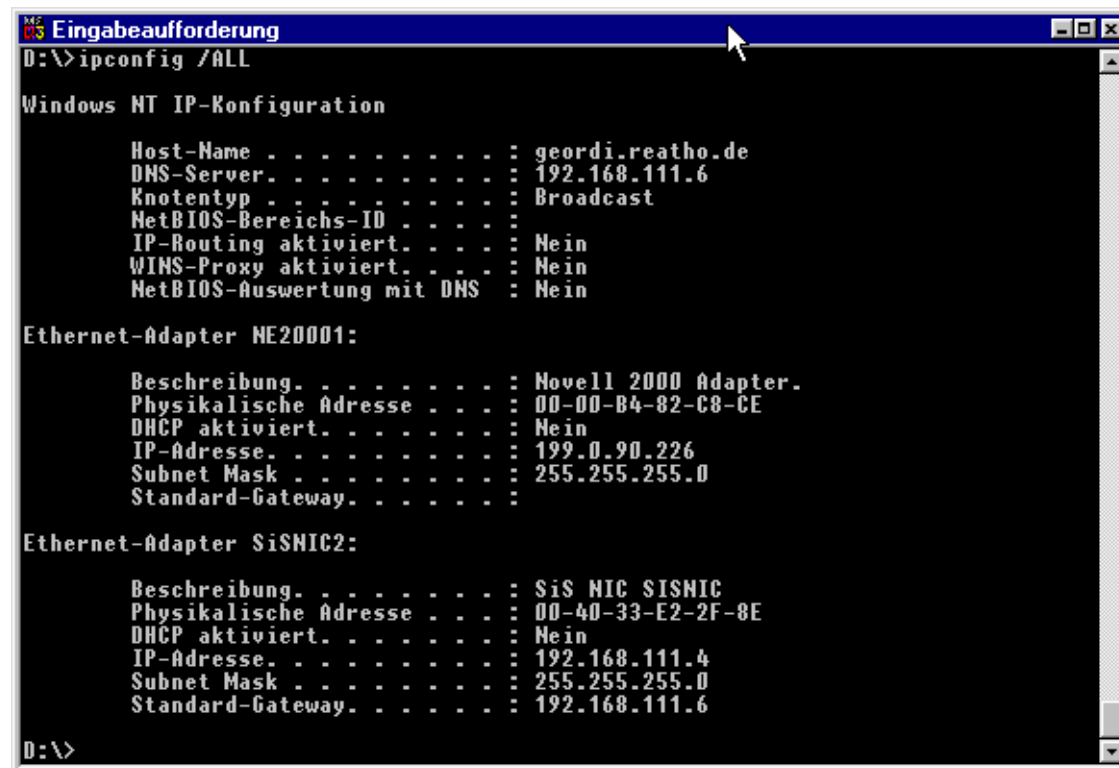
Application
TCP / UDP
IP
Physical Layer

- MAC-Adresse: 00-00-b4-82-c8-ce
IP-Adresse: 192.168.111.1 mit Netzwerkmaske ff:ff:ff:00 oder /24
TCP/UDP Ports: Eigene Port Nr. auf Sender- und Empfängerseite
- Hub: Physikalische Verbindung zwischen Netzwerkadaptern
Switch: Wie Hub, jedoch mit Filterung auf physikalischer Schicht
Router: Verbindet Netze der IP-Schicht

COMPROTware:Testtool Mithören auf dem Netz

Mithören auf dem Netzwerk

- Zusätzliche Tools des Betriebssystems:
 - ▲ Bei all diesen Tools erhält man über die Option „-?“ eine Hilfe
 - ▲ ipconfig.exe - IP Konfiguration von MS Windows



```
D:\>ipconfig /ALL

Windows NT IP-Konfiguration

    Host-Name . . . . . : geordi.reatho.de
    DNS-Server . . . . . : 192.168.111.6
    Knotentyp . . . . . : Broadcast
    NetBIOS-Bereichs-ID . . . . . :
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    NetBIOS-Auswertung mit DNS : Nein

Ethernet-Adapter NE20001:

    Beschreibung. . . . . : Novell 2000 Adapter.
    Physikalische Adresse . . . . . : 00-00-B4-82-C8-CE
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 199.0.90.226
    Subnet Mask . . . . . : 255.255.255.0
    Standard-Gateway. . . . . :

Ethernet-Adapter SiS NIC2:

    Beschreibung. . . . . : SiS NIC SiS NIC
    Physikalische Adresse . . . . . : 00-40-33-E2-2F-8E
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.111.4
    Subnet Mask . . . . . : 255.255.255.0
    Standard-Gateway. . . . . : 192.168.111.6

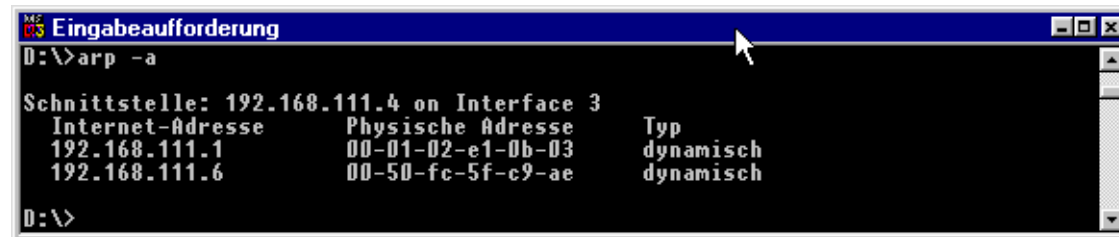
D:\>
```

COMPROTware:Testtool

Mithören auf dem Netz

Mithören auf dem Netzwerk

- arp.exe - Tabelle IP-/physikalische Adresse (Address Resolution Protocol)
Liefert Liste aller bekannten Paare



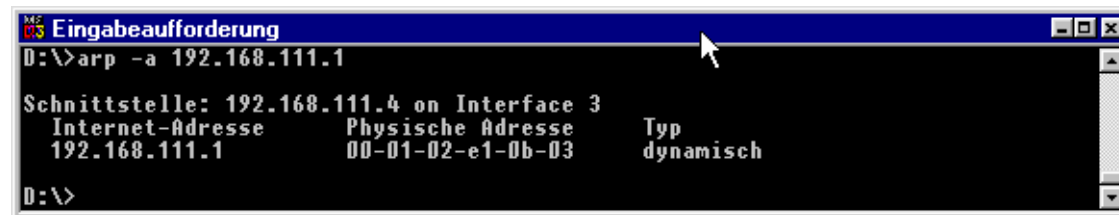
```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

D:\>arp -a

Schnittstelle: 192.168.111.4 on Interface 3
Internet-Adresse    Physische Adresse    Typ
192.168.111.1      00-01-02-e1-0b-03    dynamisch
192.168.111.6      00-50-fc-5f-c9-ae    dynamisch

D:\>
```

Oder nur die physikalische Adresse zu einer IP-Adresse



```
Microsoft Windows [Version 6.0.6002.18005]
(c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

D:\>arp -a 192.168.111.1

Schnittstelle: 192.168.111.4 on Interface 3
Internet-Adresse    Physische Adresse    Typ
192.168.111.1      00-01-02-e1-0b-03    dynamisch

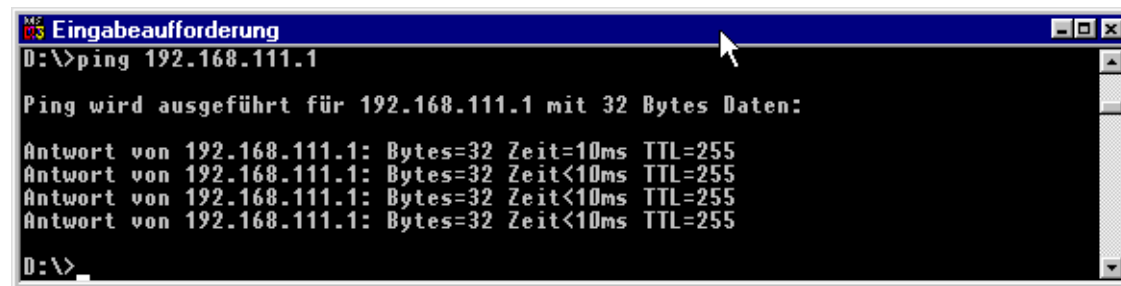
D:\>
```

COMPROTware:Testtool

Mithören auf dem Netz

Mithören auf dem Netzwerk

- ▲ ping.exe - Überprüft die Erreichbarkeit auf IP-Schicht



```
MS-DOS Eingabeaufforderung
D:\>ping 192.168.111.1

Ping wird ausgeführt für 192.168.111.1 mit 32 Bytes Daten:

Antwort von 192.168.111.1: Bytes=32 Zeit=10ms TTL=255
Antwort von 192.168.111.1: Bytes=32 Zeit<10ms TTL=255
Antwort von 192.168.111.1: Bytes=32 Zeit<10ms TTL=255
Antwort von 192.168.111.1: Bytes=32 Zeit<10ms TTL=255

D:\>
```

- ▲ pathping.exe

COMPROTware: Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- ▲ route.exe - Netzwerk-Routing-Tabelle
Welches Ziel (Host oder Netzwerk) ist via welches Gateway über welche Schnittstelle zu erreichen?

```

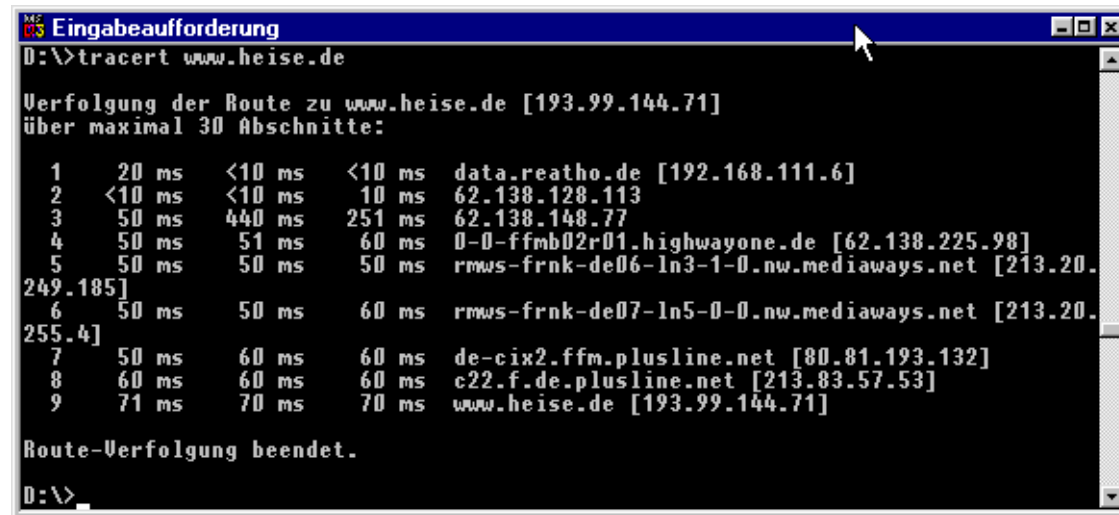
D:\>route PRINT
=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x2 ...00 00 b4 82 c8 ce ..... Novell 2000 Adapter.
0x3 ...00 40 33 e2 2f 8e ..... SiS NIC SISNIC
=====
Aktive Routen:
Netzwerk  Ziel           Netzmaske      Gateway         Schnittst.  Metrik
-----
0.0.0.0    0.0.0.0         0.0.0.0        192.168.111.6   192.168.111.4  1
127.0.0.0  255.0.0.0       255.0.0.0      127.0.0.1      127.0.0.1     1
192.168.111.0  255.255.255.0   192.168.111.4  192.168.111.4  192.168.111.4  1
192.168.111.4  255.255.255.255 127.0.0.1      127.0.0.1     1
192.168.111.255 255.255.255.255 192.168.111.4  192.168.111.4  192.168.111.4  1
199.0.90.0    255.255.255.0   199.0.90.226   199.0.90.226   199.0.90.226   1
199.0.90.226  255.255.255.255 127.0.0.1      127.0.0.1     1
199.0.90.255  255.255.255.255 199.0.90.226   199.0.90.226   199.0.90.226   1
224.0.0.0    224.0.0.0       192.168.111.4  192.168.111.4  192.168.111.4  1
224.0.0.0    224.0.0.0       199.0.90.226   199.0.90.226   199.0.90.226   1
255.255.255.255 255.255.255.255 199.0.90.226   199.0.90.226   199.0.90.226   1
=====
D:\>

```

COMPROTware: Testtool Mithören auf dem Netz

Mithören auf dem Netzwerk

- ▲ tracert.exe - Weg zu einem Host
Zeige mir alle Hosts auf dem Weg zu meinem Ziel



```
D:\>tracert www.heise.de

Verfolgung der Route zu www.heise.de [193.99.144.71]
über maximal 30 Abschnitte:

 1  20 ms  <10 ms  <10 ms  data.reatho.de [192.168.111.6]
 2  <10 ms  <10 ms  10 ms  62.138.128.113
 3  50 ms  440 ms  251 ms  62.138.148.77
 4  50 ms  51 ms  60 ms  0-0-ffmb02r01.highwayone.de [62.138.225.98]
 5  50 ms  50 ms  50 ms  rmws-frnk-de06-ln3-1-0.nw.mediaways.net [213.20.
249.185]
 6  50 ms  50 ms  60 ms  rmws-frnk-de07-ln5-0-0.nw.mediaways.net [213.20.
255.4]
 7  50 ms  60 ms  60 ms  de-cix2.ffm.plusline.net [80.81.193.132]
 8  60 ms  60 ms  60 ms  c22.f.de.plusline.net [213.83.57.53]
 9  71 ms  70 ms  70 ms  www.heise.de [193.99.144.71]

Route-Verfolgung beendet.

D:\>
```

COMPROTware:Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- ▲ netstat.exe -e
Statistik Ethernet-Frames

```

D:\>netstat -e
Schnittstellenstatistik

                Empfangen                Gesendet
Bytes                20385660                9425644
Unicast-Pakete                25865                23363
Nicht-Unicast-Pakete                3208                1824
Verworfen                0                0
Fehler                0                257
Unbekannte Protokolle                0
    
```

- ▲ netstat.exe -s
Statistik IP-Schicht

```

D:\>netstat -s
IP-Statistik

Empfangene Pakete = 28542
Empfangene Vorspannfehler = 0
Empfangene Adreßfehler = 0
Weitergeleitete Datagramme = 0
Empfangene unbekannte Protokolle = 0
Empfangene verworfene Pakete = 0
Empfangene übermittelte Pakete = 28542
Ausgabeaufforderungen = 24930
Verworfen Routing-Pakete = 0
Verworfenne Ausgabepakete = 0
Ausgabepakete ohne Routing = 0
Neuaufbau erforderlich = 0
Neuaufbau erfolgreich = 0
Neuaufbau erfolglos = 0
Erfolgreiche Datagrammfragmentierung = 0
Erfolglose Datagrammfragmentierung = 0
Erzeugte Fragmente = 0
    
```


COMPROTware:Testtool
 Mithören auf dem Netz

Mithören auf dem Netzwerk

```

ICMP-Statistik
      Empfangen  Gesendet
Nachrichten      46      46
Fehler           0       0
Ziel nicht erreichbar 0       1
Zeitüberschreitung 30       0
Parameterprobleme  0       0
Quelldrosselung   0       0
Redirects         0       0
Echos            0      45
Echo-Antworten   16       0
Zeiteinträge     0       0
Zeiteintrag-Antworten 0       0
Adreßmasken      0       0
Adreßmaske-Antworten 0       0

TCP-Statistik
Aktiv geöffnet           = 465
Passiv geöffnet         = 2
Erfolgreiche Verbindungsversuche = 2
Zurückgesetzte Verbindungen = 8
Aktuelle Verbindungen   = 4
Empfangene Segmente     = 25413
Gesendete Segmente      = 22856
Erneut übertragene Segmente = 9

UDP-Statistik
Empfangene Datagramme = 3083
Keine Anschlüsse      = 46
Empfangsfehler        = 0
Gesendete Datagramme  = 2019

D:\>
    
```

COMPROTware:Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- Typischer Verbindungsaufbau

```

11:58:36.777
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1034 -> 2404
    SeqNo=41421, AckNo=0
    Data Offset=6*32bit, Control Bits=0x02|urg ack psh rst SYN fin, Window=8192; Cksm:
    TCP Option: Kind=2|Maximum Segment Size, Length=4: 1460
11:58:36.777
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1034
    SeqNo=3813791165, AckNo=41422
    Data Offset=6*32bit, Control Bits=0x12|urg ACK psh rst SYN fin, Window=8192; Cksm:
    TCP Option: Kind=2|Maximum Segment Size, Length=4: 1460
11:58:36.777
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1034 -> 2404
    SeqNo=41422, AckNo=3813791166
    Data Offset=5*32bit, Control Bits=0x10|urg ACK psh rst syn fin, Window=8760; Cksm:
11:58:37.108
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1034 -> 2404
    SeqNo=41422, AckNo=3813791166
    Data Offset=5*32bit, Control Bits=0x18|urg ACK PSH rst syn fin, Window=8760; Cksm:

U: STARTDT act
11:58:37.108
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1034
  
```

COMPROTware:Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- Während der Verbindung

```

11:58:37.168
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1034
    SeqNo=3813791172, AckNo=41444
    Data Offset=5*32bit, Control Bits=0x18|urg ACK PSH rst syn fin, Window=8192; Cksm:

I: SSN=0, RSN=1
  C_IC_MA_1 [actcon +]      12      0  QOI=Station interrogation (global)
11:58:37.268
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1034 -> 2404
    SeqNo=41444, AckNo=3813791188
    Data Offset=5*32bit, Control Bits=0x10|urg ACK psh rst syn fin, Window=8738; Cksm:
11:58:37.278
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1034
    SeqNo=3813791188, AckNo=41444
    Data Offset=5*32bit, Control Bits=0x18|urg ACK PSH rst syn fin, Window=8192; Cksm:

I: SSN=1, RSN=1
  M_SP_MA_1 [inrogen +]    12      263  SPI=1|0n      [iv nt sb bl]
                                267  SPI=1|0n      [iv nt sb bl]

I: SSN=2, RSN=1
  M_SP_MA_1 [inrogen +]    12    10016  SPI=0|0ff      [iv nt sb bl]
                                ( 10016+1 )  SPI=0|0ff      [iv nt sb bl]
                                ( 10016+2 )  SPI=0|0ff      [iv nt sb bl]
                                ( 10016+3 )  SPI=0|0ff      [iv nt sb bl]

```

COMPROTware:Testtool
Mithören auf dem Netz

Mithören auf dem Netzwerk

- Typischer Verbindungsabbau

```

11:58:36.527
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1033
    SeqNo=3802081444, AckNo=41503
    Data Offset=5*32bit, Control Bits=0x11|urg ACK psh rst syn FIN, Window=8192; Cksm=
11:58:36.527
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1033 -> 2404
    SeqNo=41503, AckNo=3802081445
    Data Offset=5*32bit, Control Bits=0x10|urg ACK psh rst syn fin, Window=8220; Cksm=
11:58:36.527
  IP datagram: 171.26.177.141 -> 171.26.177.150
  TCP header:
    Port: 1033 -> 2404
    SeqNo=41503, AckNo=3802081445
    Data Offset=5*32bit, Control Bits=0x11|urg ACK psh rst syn FIN, Window=8220; Cksm=
11:58:36.537
  IP datagram: 171.26.177.150 -> 171.26.177.141
  TCP header:
    Port: 2404 -> 1033
    SeqNo=3802081445, AckNo=41504
    Data Offset=5*32bit, Control Bits=0x10|urg ACK psh rst syn fin, Window=8192; Cksm=
  
```

COMPROTware:Testtool Message Log-Dateien

Message Storage speichern

- Der gesamte Protokollverkehr wird während der Simulation oder des Mithörens im Message Storage gespeichert
- Der Inhalt des Message Storage kann in eine Datei geschrieben werden
- Es werden immer Rohdaten in den Message Log-Dateien gespeichert; Damit bleibt später bei der Off-line-Analyse die freie Wahl der Darstellungsweise bestehen
- Zusätzlich wird das Protokollprofil gespeichert, sodass beim Reinladen einer Datei sofort die korrekten Parameter eingestellt sind
- Der aktuelle Inhalt des Message Storage kann über *File -> Save as ...* gespeichert werden; Vergessen Sie nicht die Dateierweiterung *.mlg* beim Dateinamen im Verzeichnisdialog anzugeben

Mitschreiben

- Zusätzlich kann während der Simulation oder des Mithörens der Protokollverkehr in einer Datei mitgeschrieben werden (*File -> Log to file ...* und *File -> Close Log file*); Diese Datei kann beliebig lang werden; Damit können auch umfangreiche Protokolle über mehrere Tage hinweg erstellt werden, die sonst nicht in den Message Storage passen würden

Zugriff auf Message Log-Datei

- Durch *File -> Open from ...* kann eine Message Log-Datei wieder eingelesen werden
- Eine sehr lange Mitschrift kann durch *Extra -> Split Log file ...* in kleinere Bruchstücke zerteilt werden

COMPROTware:Testtool Off-line Analyse

Off-line Analyse

- Zur Nachbearbeitung des aufgezeichneten Protokollverkehrs
- Zur Off-line Analyse ist **keine Lizenz notwendig**
- Um in ruhiger Umgebung den Protokollverkehr im Einzelnen nochmals durchgehen zu können, zu dokumentieren und um die richtigen Schlüsse zu ziehen
- Über *File -> Open from ...* kann eine Message Log-Datei wieder eingelesen werden; Über die Cursortasten kann beliebig im Protokollverkehr navigiert und über Shortcut Keys der gewünschte Darstellungsmodus ausgewählt werden

Exportieren in Datei

- *Extra -> Export to file ...* erlaubt es, den Inhalt des Message Storage im gerade gewählten Darstellungsmodus in eine Datei zu exportieren

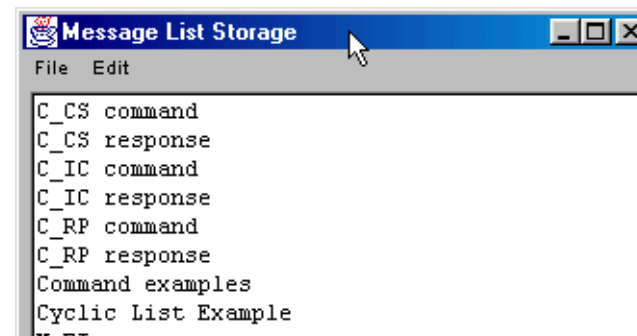
Message Storage löschen

- *Clear* im Hintergrundmenü löst das Löschen des Message Storage-Inhalts aus

COMPROTware:Testtool Message List Storage

Message List Storage

- Der Message List Storage enthält alle Nachrichtenlisten
- Über *Edit -> Message List Storage ...* kann eine Ansicht auf den Message List Storage geöffnet werden

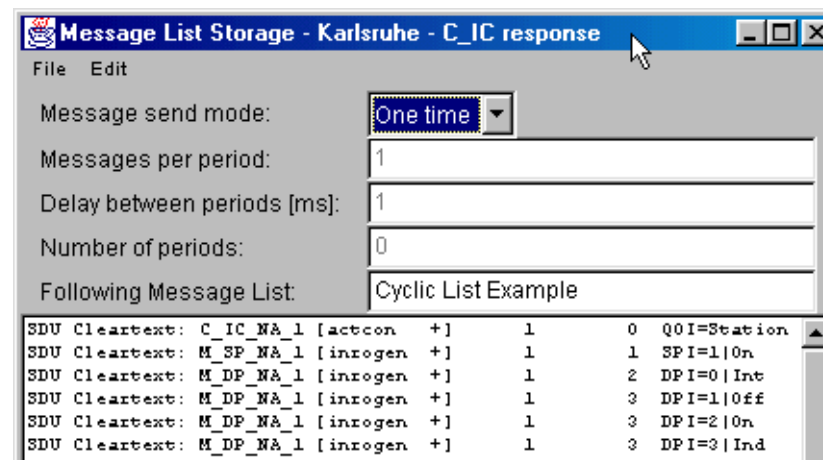


- Die Namen der Nachrichtenlisten sind frei wählbar, müssen aber eindeutig sein; Bei bestimmten Protokollen haben bestimmte Nachrichtenlistenamen eine besondere Bedeutung, z.B. enthält *C_IC response* die Antwort auf eine IEC 60870-5-101/-104-Generalabfrage
- Im Menü *File* kann über *New* eine neue (leere) Nachrichtenliste erzeugt werden, *Open from ...* liest Nachrichtenlisten ein und *Save as ...* speichert alle Nachrichtenlisten im Message List Storage in einer Datei; Das Hintergrundmenü und das Menü *Edit* erlaubt das Bearbeiten, Umbenennen, Ausschneiden, Kopieren, Einfügen, Senden und Stoppen einer Nachrichtenliste; Doppelklick auf einen Listennamen öffnet ein Bearbeitungsfenster für die Liste

COMPROTware:Testtool Nachrichtenlisten

Nachrichtenlisten

- Nachrichtenlisten können einzeln in eine Datei gespeichert (*File -> Save as ...*), Meta-Nachrichten können über *Edit* bearbeitet, kopiert, eingefügt und gelöscht werden; Doppelklick auf eine Meta-Nachricht öffnet ein Bearbeitungsfenster
- Einige Attribute und die Liste der Meta-Nachrichten bilden zusammen eine Nachrichtenliste (die Interpretation hängt vom gewählten Protokoll ab!)



- Die Attribute legen fest:
 - ▲ Ob die Liste einmal (One time) oder zyklisch abgearbeitet (Cyclic) wird
 - ▲ Bei zyklischer Abarbeitung: Wieviele Nachrichten in einer Period verschickt werden sollen, die Wartezeit zwischen den Perioden und die Anzahl der Perioden
 - ▲ Die nachfolgende Nachrichtenliste

COMPROTware:Testtool
Besondere Nachrichtenlisten

Besondere Nachrichtenlisten

- Für verschiedene Protokoll reservierte Nachrichtenlistenennamen:
 - ▲ IEC 60870-5-101/-104:
 - M_EI message - Initialisierungsnachricht (nach Verbindungsaufbau)
 - C_IC command - Generalabfrage (nach Verbindungsaufbau)
 - C_IC response - Antwort auf Generalabfrage
 - C_RP response - Antwort auf Prozessrücksetzbefehl
 - C_CS response - Antwort auf Synchronisationsbefehl
 - ▲ IEC 60870-5-102/-103:
 - Init message - Initialisierungsnachricht (nach Verbindungsaufbau)
 - GI request - Generalabfrage (nach Verbindungsaufbau)
 - GI response - Antwort auf Generalabfrage
 - ResetProcess response - Antwort auf Prozessrücksetzbefehl
 - ClockSync response - Antwort auf Synchronisationsbefehl
 - ▲ DNP3 und DNP3 over LAN/WAN:
 - GI request - Generalabfrage (nach Verbindungsaufbau)
 - Reset Device Restarted - Rücksetzen des gleichnamigen Bits
 - Timesync - Antwort auf Anforderung Zeitsynchronisation
 - Read Class1 - Antwort auf Anzeige Class 1 Daten verfügbar
 - Read Class2 - Antwort auf Anzeige Class 2 Daten verfügbar
 - Read Class3 - Antwort auf Anzeige Class 3 Daten verfügbar

Besondere Nachrichtenlisten - Fortsetzung

▲ ABB RP570/571:

Init message - Initialisierungsnachricht (nach Verbindungsaufbau)

Status Check request - Generalabfrage (nach Verbindungsaufbau)

Status Check response - Antwort auf Generalabfrage

Coldstart response - Antwort auf Prozessrücksetzbefehl (FCOM 1)

VersionId response - Antwort auf Anfrage Firmwareversion (FCOM 4)

▲ MODBUS:

Cyclic Queries - Zyklische Liste mit Anfragen

Response Read coils 1...8 - Antwort; Wertebereich anpassen

Response Read input discretes 1...8 - Antwort; Wertebereich anpassen

Response Read multiple registers 1...8 - Antwort; Wertebereich anp.

Response Read multiple registers 1...8 - Antwort; Wertebereich anp.

Response Read input registers 1...8 - Antwort; Wertebereich anpassen

Response Read exception status

Response Read general reference 1/2/3/4 - Antwort; Werte anpassen

Response Read/write registers 1...8 - Antwort; Wertebereich anpassen

Response Read FIFO queue 8 - Antwort; Wert anpassen

COMPROTware:Testtool Meta-Nachrichten

Meta-Nachrichten

- Die Nachrichtenlisten bestehen aus einzelnen Meta-Nachrichten;
Die Meta-Nachrichten können beinhalten:
 - ▲ Einen gesamten Frame (Link Layer-Telegramm) als Hexstring (PDU transparent)
 - ▲ Nutzdateninformation (Applikation Layer-Nachricht) in Klartext oder als Hexstring (SDU Cleartext oder SDU transparent)
 - ▲ Anwenderkommentar (User String)
 - ▲ Wartezeit (Delay)
 - ▲ Abrupter, unkontrollierter Abbruch der Verbindung (Abort)
 - ▲ Kontrolliertes Runterfahren der Verbindung (Shutdown)
- Die Klartexteingabe von Nachrichten bietet eine sehr schnelle und effiziente Möglichkeit, Nachrichtenlisten einzugeben

Construct IEC 60870-5-101 message:

SDU Cleartext Class: 2 Options: Send/Confirm

Type Ident: 1 M_SP_NA_1

COT: 20 inrogen

Common Address: 1 Information Object Address: 1

S/Q:
Value: 0x81 Descriptor:

QDS:
Value:

Date: 98 - 12 - 24 9 : 36 12000 ms

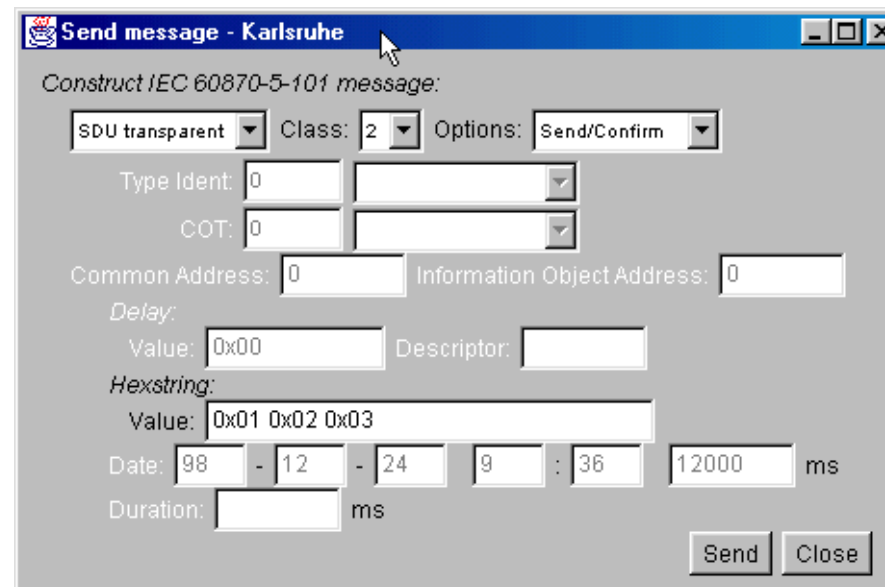
Duration: ms

Set Send Cancel

COMPROTware:Testtool Nachrichten einzeln senden

Nachrichten einzeln senden

- Neben der Möglichkeit, Nachrichtenlisten zu bearbeiten und zu versenden, können auch Nachrichten einzeln verschickt werden;
Dazu dient *Send message ...* im Hintergrundmenü des Darstellungsfensters



- Vorteil hier ist, dass die Eingabefelder schnell verändert und sofort die Nachricht verschickt werden kann

COMPROTware:Testtool Benutzerkommentare

Benutzerkommentare

- Über das Fenster „Send Message“ können auch Benutzerkommentare eingefügt werden:

Send message - Unknown

Construct IEC 60870-5-104 message:

User String: [dropdown] Class: 1 Options: Send/Confirm

Type Ident: 9 M_ME_NA_1

COT: 1 per/cyc Pos.Con. No Test

Common Address: 1 Information Object Address: 15

String:
Value: Test 64.3 Descriptor:

QDS:
Value: 0x01

Date: Edit Date&Time
3 - 8 - 11 14 : 31 39569 ms

Duration: ms

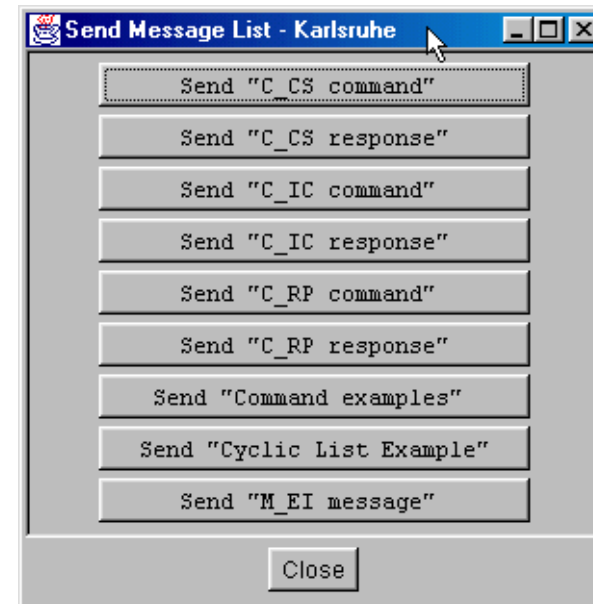
Send Close

Diese werden sofort in den Message Storage eingefügt

COMPROTware:Testtool Nachrichtenlisten senden

Nachrichtenlisten senden

- Ein eigenes Fenster erlaubt es einfach, Nachrichtenlisten auszulösen und deren Abarbeitung zu stoppen; Dazu im Hintergrundsmenü *Send Message List ...* auswählen:



- Es können mehrere Nachrichtenlisten gleichzeitig in Abarbeitung sein; Aber jede Nachrichtenliste kann gleichzeitig nur einmal abgearbeitet werden
- Durch *Send* wird die Abarbeitung gestartet, *Stop* beendet sie

COMPROTware:Testtool Konfigurationen vorbereiten

Konfigurationen vorbereiten

- Konfigurationen können bequem am Schreibtisch vorbereitet und dann abgespeichert werden; Damit kann ein wesentlicher Schritt zur Vorbereitung eines Einsatzes bereits im Vorfeld erledigt werden
- Zu einer Konfiguration gehört: Protokollprofil, Geladene **User Engine Classes**, Allgemeine Einstellungen und Position/Größe des Fensters
- Speichern der Konfigurationen mittels *File -> Save Configuration as ...*, Einlesen der Konfiguration entsprechend mittels *File -> Open Configuration from ...*
- Wenn **CPTT** mehrfach mit gleicher Konfiguration auf dem Desktop laufen sollen, dann einfach einmal **CPTT** starten, Konfiguration einstellen und dann mittels *File -> Save Configuration to user default* speichern; Die neue Benutzerkonfiguration ist gespeichert; Jetzt **CPTT** weitere Male starten ... alle **CPTTs** haben die gleiche Konfiguration

COMPROTware:Testtool User Engine Classes

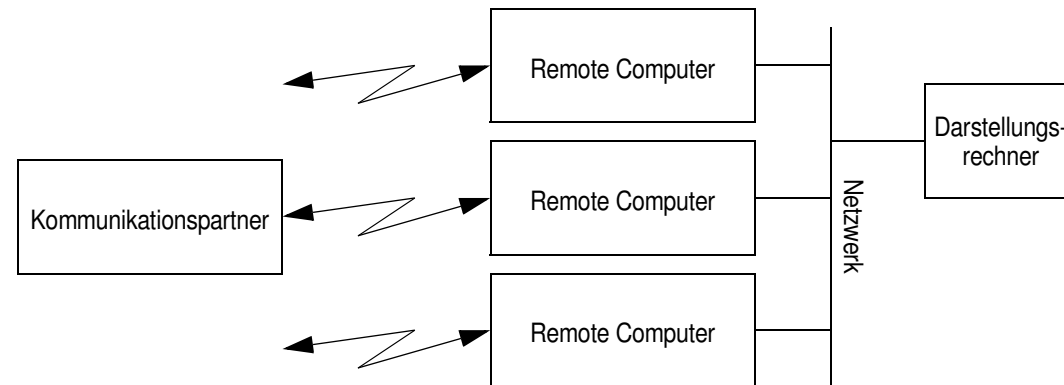
User Engine Classes

- Sind Plug-ins zu **CPTT**, die in Java implementiert sind. Im Programmer's Guide ist die API zu den **User Engine Classes** beschrieben; Voraussetzung für die Entwicklung von **User Engine Classes** ist ein installiertes Java Development Kit
- Da Java sehr ähnlich zu ANSI C und C++ ist, fällt es leicht, **User Engine Classes** zu schreiben
- Java dient zur Sicherung des Programms gegen Abstürze von **User Engine Classes**
- Ein Beispiel für **User Engine Classes** wird mitgeliefert:
IEC 60870-5-101/-104-Filetransfer
- Über *Edit -> User Engine Classes ...* können **User Engine Classes** ausgewählt und geladen werden; Wird der Pfad gelöscht, dann wird die Klasse wieder entfernt
- Viele weitere Anwendungen sind denkbar:
 - ▲ Filetransfer und andere Application Layer Prozeduren
 - ▲ Nachbilden von gerätespezifischen Pseudopunkten
 - ▲ Überprüfen der Grundfunktionen eines Geräts

COMPROTware:Testtool
Remote I/O Server

Remote I/O Server

- Der **RIO Server** löst das Problem, dass mit **CPTT** Datenströme analysiert und dargestellt werden sollen, die nicht direkt am Darstellungsrechner vorliegen. Der **RIO Server** tauscht dabei über eine Kommunikationsschnittstelle (Serielle Schnittstelle, Netzwerk, Datei) des Remote Computers Datentelegramme mit einem Kommunikationspartner aus. Die Datentelegramme werden über das Netzwerk an **CPTT** weitergereicht um dort analysiert und dargestellt zu werden.



- Der **RIO Server** ist ein eigenständiges Programm, das getrennt von **CPTT** auf einem anderen Rechner läuft. Während **CPTT** auf MS Windows-Rechnern beschränkt ist, läuft der leichtgewichtige **RIO Server** auf vielen Rechnerarchitekturen (MS Windows, Linux, Solaris, ...).

COMPROTware:Testtool
Remote I/O Server
RIO Server

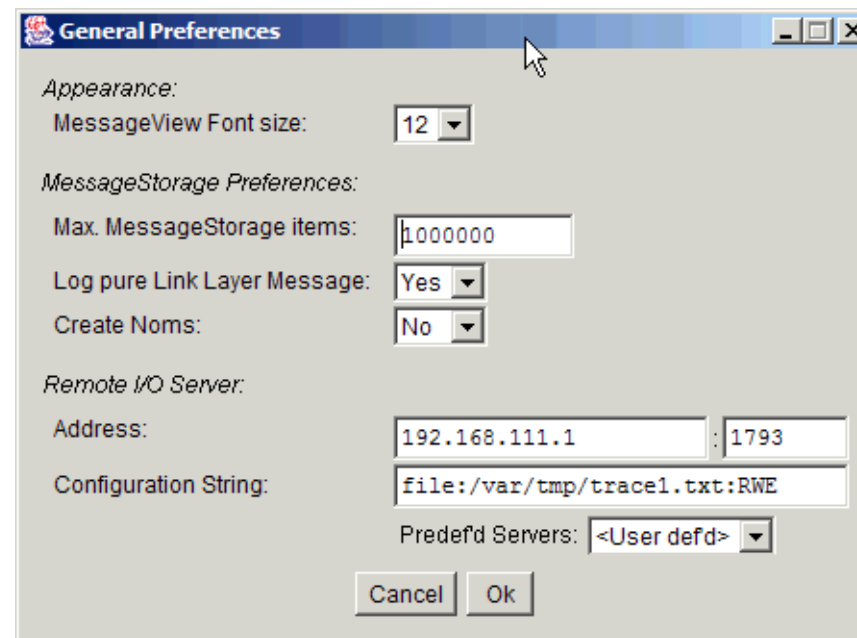
RIO Server

- Die ausführbare Fassung des **RIO Servers** für die benötigte Rechnerarchitektur ist auf der CD-ROM im Verzeichnis \CPRioServer zu finden:
 - ▲ CPRioServer_iX86_WIN32 für MS Windows
 - ▲ CPRioServer_iX86_Linux für PC Linux 2.x
 - ▲ CPRioServer_sun4_SunOS_5 für Sun SPARC Solaris 7
- Kopieren Sie die ausführbare Fassung auf Ihr Zielsystem.
- Der **RIO Server** wird einfach auf dem Remote Computer gestartet. Damit der **RIO Server** immer zur Verfügung steht, sollte er gleich beim Hochfahren des Rechners oder beim Start der zu überwachenden Applikation ausgeführt werden:
 - ▲ Unter MS Windows: RIO Server in Registry eintragen
 - ▲ Unter UNIX oder Linux innerhalb der /etc/rd.d Skripte
 - ▲ Oder durch ein Skript in Verbindung mit der zu überwachenden Applikation

COMPROTware:Testtool
Remote I/O Server
RIO Client in CPTT

RIO Client in CPTT

- Die Konfiguration des *RIO Clients* in *CPTT* erfolgt über *Edit->General Preferences*:



- In diesem Fenster wird die Adresse (Rechnername oder IP-Adresse) des *RIO Servers*, die TCP Port No. und die Konfigurationszeichenkette eingetragen. Die Konfigurationszeichenkette muss aus Sicht des *RIO Servers* angegeben werden (siehe unten).

COMPROTware:Testtool
Remote I/O Server
RIO Client in CPTT

RIO Client in CPTT

- Für die Eingaben gilt:
 - ▲ Ist eine korrekte **RIO Server**-Adresse eingetragen, dann erfolgt ab sofort die Kommunikation über den **RIO Server**. Soll wieder ohne **RIO Server** gearbeitet werden, dann einfach die Adresse löschen.
 - ▲ Wurden vordefinierte Konfigurationen (als CPTT-Konfigurationsdatei) eingelesen, dann können diese unter *Predef'd Servers* ausgewählt und die übernommen werden.
- „@Rio“ in der Titelzeile des Fensters zeigt an, dass die Kommunikation indirekt über einen **RIO Server** erfolgt.
- Vordefinierte **RIO Server**-Konfiguration können über *File->Open Configuration from ...* eingelesen werden. Die Pflege dieser Konfigurationen muss über einen externen Editor erfolgen.
- Die Konfigurationszeichenketten haben folgenden Aufbau:

<Medium>:<Ort>[;<Ort>]:<Format>

 - ▲ dblsr1:com1,9600,8n1;com2,9600,8n1:PPP
Von zwei seriellen Schnittstellen (com1 und com2 mit jeweils 9600 Baud, 8 Daten-, 1 Stopp- und keinem Paritätsbit) im Format PPP (Point-to-Point Protocol) werden sukzessive PPP-Telegramme empfangen und an **CPTT** weitergegeben.
 - ▲ file:/var/tmp/trace1.txt;/var/tmp/trace2.txt:RWE
Aus einer Datei, Dateipfad und Name ist „/var/tmp/trace1.txt“ bzw. „/var/tmp/trace2.txt“, im Format RWE werden sukzessive alle hinzugekommenen Datentelegramme ausgelesen und an **CPTT** weitergegeben.

COMPROTware:Testtool Wir haben gesehen ...

Wir haben gesehen ...

- Wie über *Edit -> Protocol Profiles ...* aus einer Protokollfamilie ein Protokoll ausgewählt und dessen Profil festgelegt wird,
- die Protokollsimulation als Controlling Station/Master oder als Controlled Station/Slave durch *Action -> Simulate Controlling Station/Simulate Master* bzw. *Action -> Simulate Controlled Station/Simulate Slave* gestartet wird,
- die Simulation über *Action -> Stop* wieder beendet werden kann,
- die Darstellungweise des Protokollverkehrs mittels *Hintergrundmenü* (rechte Maustaste) -> *Formatting Options ...* verändert und
- der Nachrichtenspeicher auf Platte gesichert (*File -> Save as ...*) und wieder eingelesen (*File -> Open from ...*) wird

- Die Größe des Nachrichtenspeichers ist über *Edit -> General Preference* einstellbar, ebenso, ob alle Link Layer-Informationen gespeichert werden sollen
- Für Langzeittests kann der Protokollverkehr über *File -> Log to file ...* direkt in eine Datei geschrieben werden, beendet wird das Mitschreiben über *File -> Close Log file*
- Dies ist besonders beim Mithören (*Action -> Monitor* und *Action -> Stop*) sehr hilfreich

- Lange Message Log-Datei können über *Extra -> Split Log file ...* in kleinere Teile aufgesplittet,
- der Inhalt des Nachrichtenspeichers über *Extra -> Export to textfile ...* entsprechend des gewählten Darstellungsmodus in eine Textdatei gespeichert werden

COMPROTware:Testtool
Wir haben gesehen ...

Wir haben gesehen ... - Fortsetzung

- Nachrichtelisten werden unter *Edit -> Message List Storage ...* bearbeitet, **User Engine Classes** (Plug-ins) können über *Edit -> User Engine Class ...* zu **CPTT** hinzugefügt werden
- Bei Fragen gibt *Help -> About* Ihnen die Kontaktinformationen um uns zu erreichen!

Real Thoughts GmbH

Haid-und-Neu-Straße 7

76131 Karlsruhe

Germany

Fon +49-721-6276730, Fax +49-721-6276731

Website www.realthoughts.de

E-Mail info@realthoughts.de