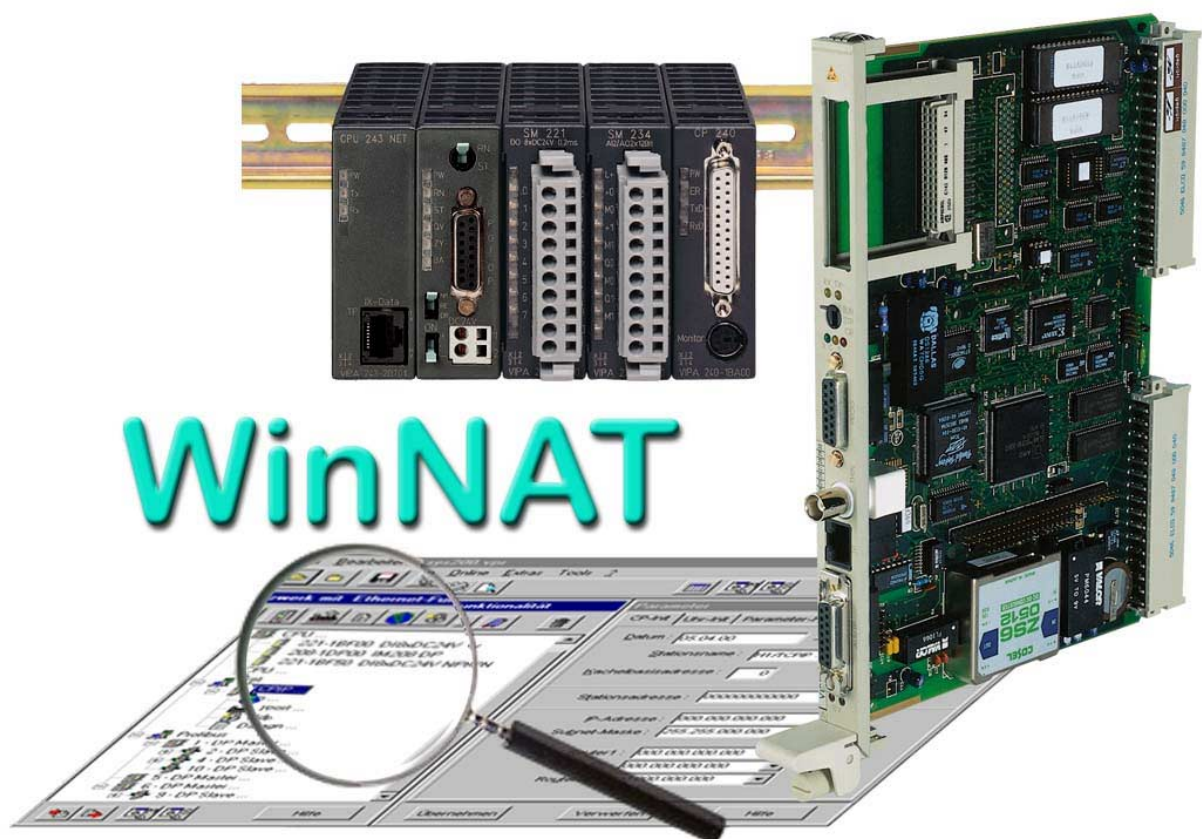

Handbuch

WinNAT

Rev. 00/32



Die Angaben in diesem Handbuch erfolgen ohne Gewähr. Änderungen des Inhalts können jederzeit ohne Vorankündigung erfolgen. Die in diesem Handbuch beschriebene Software unterliegt den Bedingungen eines allgemeinen Lizenzvertrags. Sie haben eine Kopierlizenz, die Sie berechtigt, Sicherheitskopien anzufertigen. Nach der Registrierung ist WinNat nur auf dem Rechner lauffähig für den Sie die Registrierung durchgeführt haben. Die mutwillige Deaktivierung der Registrierfunktion verpflichtet zu Schadenersatz.

© Copyright 2000 VIPA, Gesellschaft für Visualisierung und Prozeßautomatisierung mbH,
Ohmstraße 4, 91074 Herzogenaurach
Tel.: +49 (9132) 744 -0
Fax.: +49 (9132) 744 -144
EMail: info@vipa.de
<http://www.vipa.de>

Hotline: +49 (9132) 744 -114

Alle Rechte vorbehalten

VIPA® ist eingetragenes Warenzeichen der VIPA Gesellschaft für Visualisierung und Prozeßautomatisierung mbH

WINDOWS® ist eingetragenes Warenzeichen der Microsoft Corp.

WINDOWS 95® ist eingetragenes Warenzeichen der Microsoft Corp.

WINDOWS NT® ist eingetragenes Warenzeichen der Microsoft Corp.

Alle ansonsten im Text genannten Warenzeichen sind Warenzeichen der jeweiligen Inhaber und werden als geschützt anerkannt.

Änderungen im Sinne des technischen Fortschritts vorbehalten.

Inhaltsverzeichnis

Einleitung	3
Willkommen	3
Erste Schritte.....	3
Lieferumfang	3
Systemanforderung.....	3
Installation WinNAT	4
Registrierung und Freischaltung.....	4
Installation des Treibers	5
Einrichten des Netzwerks	5
Verzeichnisstruktur WinNAT.....	6
Programm Starten.....	6
Programm Beenden	6
WinNAT-Umgebung	7
Hilfesystem	7
Kontextmenü.....	7
Hauptfenster.....	8
Menüleiste	8
Menüpunkte des Hauptfensters	8
Druckerausgabe	9
Druckoptionen	9
Netzwerkanalyzer	10
Allgemeines zum Netzwerkanalyzer	10
Leistungen des Netzwerkanalyzer	10
Anwahlmöglichkeiten im Netzwerkanalyzer	10
Prinzipielle Arbeitsweise	11
WinNAT-Struktur.....	12
Aufzeichnung.....	13
Telegramme aufzeichnen.....	14
Aufzeichnung Stoppen	14
Aufzeichnung Löschen.....	14
Langzeitaufzeichnung.....	15
Analyse	16
Analyse von Telegrammen.....	17
Detailanalyse.....	18
Parameter	19
Allgemein	19
Darstellung	20
ISO-Protokoll	21
Aufzeichnung	22
Filter.....	23
Stationen (Hardwarefilter).....	23
Protokolle (Softwarefilter).....	24
TPDU (Softwarefilter).....	24
Adressen (Softwarefilter)	25
Symbol-Manager	26
Übersicht Protokolle	28
Glossar	29
Index	31

Einleitung

Willkommen

Die vorliegende Software WinNAT ist ein auf Ethernet basierender Netzwerkanalyzer.

WinNAT steht für Windows Network-Analyzer-Tool. Der Analyzer läuft unter dem Betriebssystemen Windows NT4. Wir wünschen Ihnen viel Erfolg beim Arbeiten mit WinNAT.

Erste Schritte

Lieferumfang

Das Programm WinNAT besteht aus den folgenden Komponenten :

- WinNAT
- BDE (Borland Database Engine)
- WinNAT-Treiber
- Handbuch

Systemanforderung

Für den Betrieb von WinNAT auf Ihrem Rechner ist folgende Hardware erforderlich:

- IBM- oder kompatibler PC, lauffähig unter Windows NT
- Mindestens 80486 Prozessor oder höher
- 16 MB RAM Arbeitsspeicher, besser 64 MB
- Bildschirmauflösung 800x600 oder höher, 65536 Farben
- Festplatte 100 MB und größer.
- Windows NT4
- 1 freier Steckplatz für die Netzwerkkarte

Installation WinNAT

Die Installation von WinNAT wird durch ein Setup-Programm unterstützt. WinNAT ist Bestandteil der VCL (VIPA Component Library) und kann im Rahmen des VCL-Setups installiert werden.

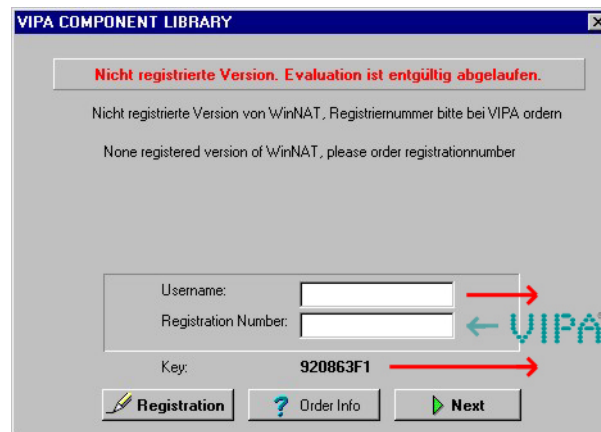
Für die Installation von WinNAT beenden Sie alle Windows-Programme, bevor Sie das Setup ausführen. Legen Sie die WinNAT-CD ein und führen das Programm Setup.exe aus. Es werden die folgenden Schritte durchgeführt:

- Der Setup Assistent wird vorbereitet, wählen Sie eine Setup-Sprache aus und bestätigen Sie mit [OK]
- Es öffnet sich das Fenster *Willkommen*. Hier erhalten Sie Informationen zur Installation und zum Urheberrecht - bestätigen Sie mit [Weiter] und stimmen Sie mit [JA] dem Lizenz-Vertrag zu.
- Tragen Sie in den *Benutzerinformationen* Ihren Namen und den Namen Ihrer Firma ein.
- Als *Zielpfad* wählen Sie das Verzeichnis für WinNAT an .
- Der Kopiervorgang installiert alle Dateien von WinNAT und der BDE auf Ihren Rechner.
- Registrierung und Freischaltung

Registrierung und Freischaltung

Bei der hier vorliegenden Version von WinNAT handelt es sich um eine 3-Tage-Testversion, die über den VIPA-Support unverzüglich freigeschaltet werden kann, d.h. Sie haben 3 Tage eine Vollversion zu Testzwecken. Nach 3 Tagen ist WinNAT nur eingeschränkt nutzbar und kann durch ein Registrierung bei VIPA freigeschaltet werden.

Starten Sie hierzu WinNAT. Es öffnet sich ein Dialogfenster in dem unter "Key" ein Schlüsselwort angezeigt wird:



Senden Sie dieses Schlüsselwort (Key) zusammen mit einem gewünschten Benutzernamen (Username) als EMail an folgende Adresse mit dem Wunsch um Freischaltung: support@vipa.de oder rufen Sie die Hotline an.

Sie erhalten umgehend per EMail für den angegebenen Benutzernamen Ihre Registration-Number.

Starten Sie WinNAT und geben Sie im Dialogfenster den "Username" und die "Registration-Number" ein und klicken Sie auf die Schaltfläche "Registration".

Sofern alle Eingaben richtig sind, wird WinNAT gestartet und ist nun voll funktionsfähig.

Installation des Treibers

Mit WinNAT wird ein spezieller Treiber mitgeliefert. Dieser Treiber enthält alle Funktionen für die Kommunikation zwischen WinNAT und einer Netzwerkkarte.

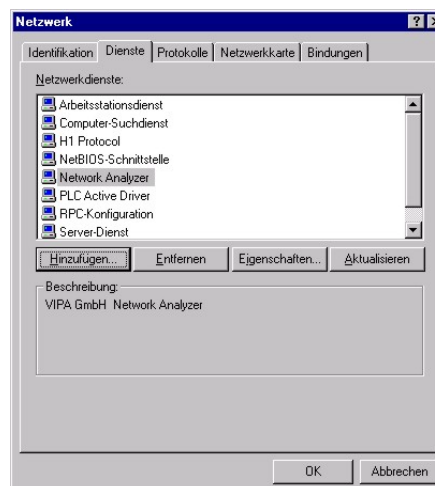
Der Treiber ist unter WINDOWS-NT4 zu installieren und ist nur in diesem Betriebssystem einsetzbar. Die Installation ist über die **Netzwerkumgebung**, die in der **Systemsteuerung** zu finden ist, durchzuführen.



Klicken Sie mit der rechten Maustaste auf die **Netzwerkumgebung** und rufen Sie *Eigenschaften* auf. Es öffnet sich ein mehrseitiges Dialogfenster. Gehen Sie auf das Register *Dienste* und fügen Sie den mitgelieferten WinNAT-Treiber hinzu.

Klicken Sie hierzu auf [Hinzufügen]. Es öffnet sich das Dialogfenster "Auswahl Netzwerkdienst". Klicken Sie auf [Diskette] und verweisen Sie auf Ihr CD-ROM-Laufwerk mit dem Verzeichnis-Pfad \NatDrv\WinNT.

Wählen "VIPA GmbH Network Analyzer" in der Liste an und klicken Sie auf [OK]. Der Network Analyzer-Dienst ist jetzt eingetragen.



Klicken Sie auf [OK] und starten Sie Ihren Rechner neu.

Einrichten des Netzwerks

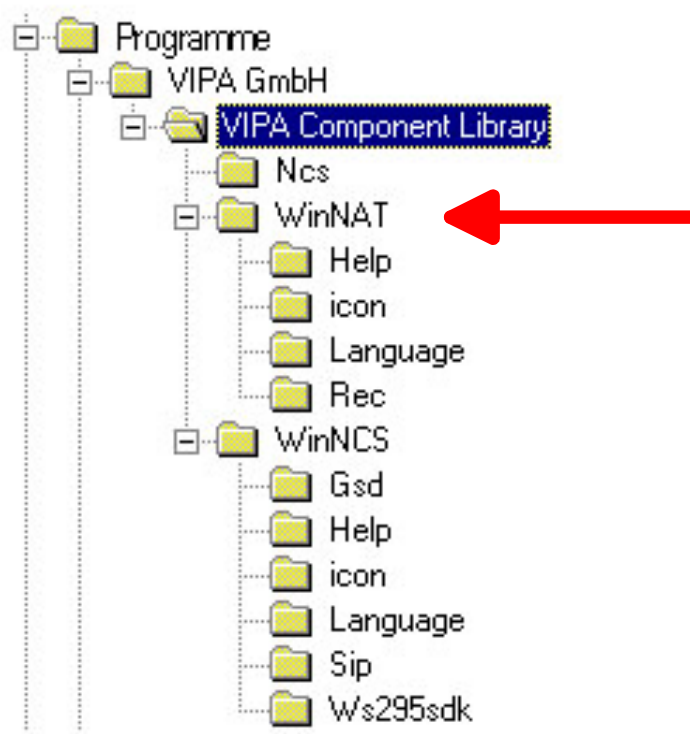
Für den Betrieb von WinNAT müssen Sie Ihren Computer an ein Ethernet-Netzwerk anbinden. Hierzu ist eine Netzwerkkarte erforderlich, die als Hardware-Komponente bei Ihrem Betriebssystem anzumelden ist.

In der **Systemsteuerung** unter *Netzwerk* finden Sie die aktuelle Netzwerkconfiguration. Falls noch nicht vorhanden, fügen Sie die Netzwerkkomponenten für das *TCP/IP-Protokoll* hinzu. Außerdem muß der Netzwerkkomponente TCP/IP unter "Eigenschaften" eine IP-Adresse zugewiesen werden. Die IP-Adressen des Analyse-Rechners und der zu analysierenden Netzwerkteilnehmer müssen in der selben Netzwerkklasse liegen, damit sie deren Kommunikationsaktivitäten aufzeichnen können.

Die IP-Adresse und nähere Angaben zum Einrichten Ihrer Netzwerkkarte erhalten sie von Ihrem Systemadministrator.

Verzeichnisstruktur WinNAT

Das Verzeichnis für WinNAT wird bei der Installation im Setup festgelegt. Bei der Installation wird die folgende Verzeichnisstruktur auf Ihre Festplatte übertragen.



Programm Starten

Aufgerufen wird WinNAT am einfachsten, indem Sie im START-Menü von WINDOWS unter "VIPA Component Library" *WinNAT* anwählen. Es ist auch möglich das Programm über die Datei *WinNAT.EXE* aufzurufen.

Sofern Sie WinNAT nicht registriert haben, erscheint beim Programmstart ein Hinweis für die Registrierung.

Das Programm beginnt die Ausführung mit dem Startfenster, das Informationen zur Version beinhaltet. Um mit WinNAT optimal arbeiten zu können, sollten Sie unter "Anzeige" in der Systemsteuerung des Betriebssystems als Schriftgrad *Kleine Schriftarten* einstellen und eine Auflösung größer oder gleich "800x600" Pixel wählen. Um die farblich unterschiedlich dargestellten Ausgaben besser unterscheiden zu können, stellen Sie 65535 Farben ein.

Programm Beenden

Beendet wird WinNAT über das Hauptmenü. Beim Beenden wird eine Datei mit dem Namen *WinNAT.ini* abgespeichert. *WinNAT.ini* beinhaltet alle Einstellungen die Sie zuvor im Programm vorgenommen haben.

WinNAT-Umgebung

Hilfesystem

WinNAT bietet vielfältige Hilfsfunktionen an. Während der Parametrierung haben Sie immer Zugriff auf alle Hilfetemen, die Sie im Hauptmenü unter dem Menüpunkt ? finden.

Immer wenn Sie im WinNAT-Fenster Hilfe benötigen, drücken Sie im entsprechenden Fenster oder einer Eingabemaske die Funktionstaste F1 oder den Hilfe-Button. Daraufhin öffnet sich kontextbezogen das Hilfefenster mit dem Hilfetext.

Mit dem Aufruf von Hilfetemen wird ein Hilfefenster geöffnet, das eine Übersicht der Hilfetemen nach Kategorie geordnet zu diesem Programm auflistet. Durch Anklicken eines Buchsymbols können Sie zu ihrem gesuchten Thema gelangen. Ein Buch kann wiederum Bücher beinhalten.

Durch Doppelklick auf ein Thema können Sie den Hilfetext zu dem Thema lesen. Durch Doppelklick auf ein geöffnetes Buch können Sie dieses wieder schließen.

Für eine Begriffsuche in den Hilfetexten haben Sie in dem Dialogfenster die Möglichkeit, den Begriff direkt einzugeben oder im Index zu suchen.

Näheres zum Hilfesystem finden Sie auch in der Beschreibung zu Ihrem Windows-System oder durch Drücken von F1 in Ihrem Hilfefenster.

Kontextmenü

Da WinNAT nach Windows-Konventionen programmiert ist, bietet das Programm auch ein Kontextmenü an, das über die rechte Maustaste aktiviert werden kann.

Über dieses Menü haben Sie direkt Zugriff auf Funktionen, die nur an dieser Mausposition möglich sind.

Über das Kontextmenü können Sie je nach Mausposition:

- Parameter einstellen
- Filter einstellen

Hauptfenster

Das Hauptfenster wird nach dem Starten von WinNAT angezeigt. Es enthält die Menüleiste und die Symbolleiste, die mit den wichtigsten Funktionen belegt ist.



Menüleiste

In der Menüleiste stehen Ihnen alle Hauptfunktionen zur Verfügung. Die Menüleiste befindet sich am oberen Rand des Hauptfensters. Die folgende Tabelle enthält eine Übersicht der Menübefehle:

Menü	Befehle
Datei	Capturefile öffnen/speichern, Druckoptionen, Beenden
Bearbeiten	Symbolik (Symbol-Manager)
Extras	Deutsch, Englisch
Analyzer	Netzwerk, Parameter, Filter
?	Hilfethemen, Info, Registration

Menüpunkte des Hauptfensters

Nachfolgend sind die Menüpunkte mit der zugehörigen Schaltfläche und einer kurzen Funktionsbeschreibung aufgeführt. Die wichtigsten Funktionen können Sie über Schaltflächen aufrufen.



Datei > Capturefile öffnen

Eine bestehende Datei mit Analyse-Aufzeichnungen wird geöffnet. Hierzu erscheint ein Dateiauswahlfenster, in dem eine Analyse-Datei ausgewählt werden kann.



Bearbeiten > *Symbolik*

Der Symbol-Manager dient der Zuweisung von symbolischen Namen zu absoluten Adressen. Hierbei kann es sich um Ethernet- oder IP-Adressen handeln.



Analyzer > Aufzeichnungsfenster *-Funktionen*

Hiermit gelangen Sie in das Aufzeichnungsfenster und können sofort mit der Aufzeichnung beginnen.

Extras > Deutsch bzw. **Extras** > Englisch

Hier können Sie ohne das Programm zu beenden die gewünschte Sprache im Programm einstellen. Zur Zeit haben Sie die Auswahl zwischen Deutsch und Englisch.

Druckerausgabe

Die Druckerausgabe dient der Dokumentation und der Fehlersuche in Ihren Aufzeichnungen. Die Druckfunktionen finden Sie als Schaltfläche in jedem WinNAT-Fenster. Sie haben so vielfältige Möglichkeiten für den Ausdruck Ihrer aufgezeichneten Daten. Hierbei können Sie auch eine bestimmte Anzahl von Frames drucken.

Druckoptionen

Über Druckoptionen können Sie Einstellungen zu Ihrem Projekt vornehmen. Bei Anwahl von **Datei > Druckoptionen** öffnet sich das Dialogfenster "Druckoptionen".



Projekt, Name, Firma,

Optional können Sie Angaben machen, die als Druckfuß in Ihrem Ausdruck erscheinen.

Netzwerkanalyzer

Allgemeines zum Netzwerkanalyzer

Der Netzwerkanalyzer für Windows NT ist ein Netzwerk-, Analyse- und Protokollierwerkzeug für Ethernet-Netzwerke. Zusammen mit einer Netzwerkkarte betrieben, stellt WinNAT ein leicht zu bedienendes Programm dar, das auf dem Betriebssystem Windows NT basiert.

Leistungen des Netzwerkanalyzer

- Übersicht über die zur Zeit laufenden Aktivitäten auf dem Netzwerk.
- Historische Aufzeichnung der Netzwerk-Aktivität über einen bestimmten Zeitraum.
- Langzeitaufzeichnung
- Liste, der am Netzwerk aktiv beteiligten Stationen.
- Übersicht, welche Stationen kommunizieren und welche Daten ausgetauscht werden.
- Sie betrachten die Telegramme einer Aufzeichnung übersichtlich in Listenform mit Kurzbeschreibung.
- Einzelne Telegramme können detailliert in einer Klartextanzeige ausgegeben werden.
- Während aufgezeichnet wird, können Sie Ihren Computer für andere Applikationen benutzen.
- Es können Hardware- (Aufzeichnungsfiler) und Softwarefilter verwendet werden.
- Zum Lieferumfang gehört die Dekodierung des ISO-TP4-Protokolls (SINEC H1 von Siemens) und TCP/IP.

Anwahlmöglichkeiten im Netzwerkanalyzer

- Alle Einstellungen werden automatisch gesichert.
- Telegramme lassen sich in verschiedenen Detailstufen anzeigen und ausdrucken.
- Aufzeichnungen können auf Festplatte gespeichert und wieder geladen werden.
- Über den Symbolmanager können symbolische Adressnamen vergeben werden.
- Es können hardwarenahe Filter für die Aufzeichnung verwendet werden.
- Es stehen vielfältige Softwarefilter für die Anzeige zur Verfügung.
- Die Größe des Aufzeichnungspuffers ist variabel.

Prinzipielle Arbeitsweise

Durch den Anschluß der Netzwerkkarte an das lokale Netz gelangen alle Telegramme in die Netzwerkkarte. Der installierte Kartentreiber transferiert die Telegramme in den Protokolltreiber. Hier werden die Aufzeichnungsfiler aktiv, die nur die Telegrammdateien der gefilterten Stationen passieren lassen. Diese Daten werden in einem Ringpuffer gespeichert. Beim Übertragen in den Puffer werden Absender und Empfänger eines Telegramms analysiert und die Aufzeichnungsliste wird aufgebaut.

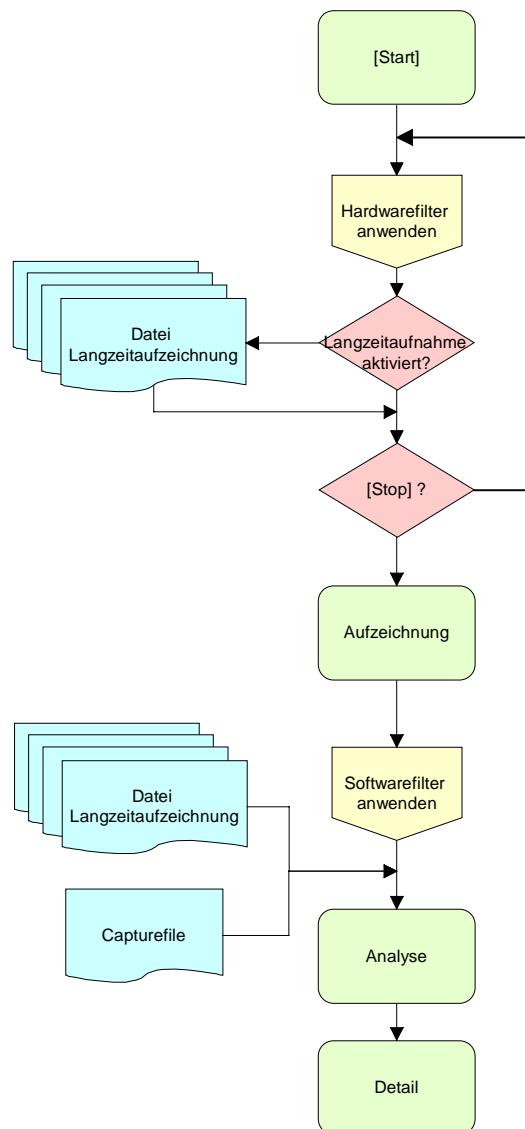
Nach dem Stoppen der Aufzeichnung kann die Aufzeichnungsliste der Stationen analysiert werden. Für die Betrachtung der aufgezeichneten Telegramme können Sie die Anzeigefiler (Softwarefilter) aktivieren. Die Telegrammanalyse zeigt die Telegramme in ihrer zeitlichen Reihenfolge an.

Mit den Bild- und Pfeiltasten oder mit der Maus können Sie in den Analyse-Listen blättern.

Ein Analysedurchgang besteht aus 3 Stufen: Aufzeichnung → Analyse → Detailanalyse

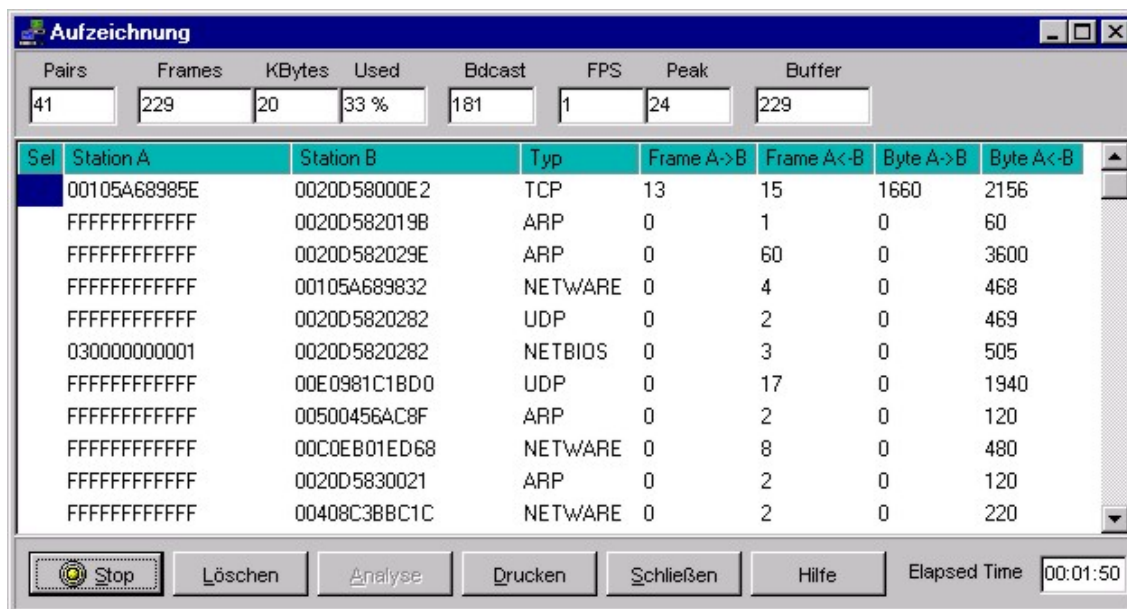
Gestartet wird eine Aufzeichnung immer in der Aufzeichnungsebene. Alle im Netzwerk an der Kommunikation beteiligten Stationspaare werden bei der Aufzeichnung erfasst und in der Aufzeichnungsliste angezeigt. Von dieser Liste ausgehend kann in die Analyse bzw. Detailanalyse verzweigt werden.

Die nachfolgenden zwei Flussdiagramme sollen dies nochmals verdeutlichen:



Aufzeichnung

Im Aufzeichnungsfenster erhalten Sie eine Liste aller Stationspaare, und eine Statistik über das Telegrammaufkommen in Ihrem Netzwerk.



Nach Betätigung der Schaltfläche [Start] wird die Aufzeichnung gestartet. Dies wird durch einen Indikator auf der Schaltfläche [Start/Stop] angezeigt. Ist die Netzwerkkarte an ein intaktes Netz angeschlossen, werden sofort alle Stationen angezeigt die zur Zeit im Netz kommunizieren. Die Stationsliste kann jederzeit durch [Löschen] gelöscht werden. Nach dem Löschen wird sie bei aktivierter Aufzeichnung sofort wieder mit den aktuellen Stationsnamen aufgebaut. Ist die symbolische Adressierung aktiviert, wird die Stationsadresse symbolisch angezeigt. Während der Aufzeichnung können Sie keine Analyse von Telegrammen aktivieren.

Nach dem Stoppen der Aufzeichnung haben Sie die Möglichkeit, die Aufzeichnung zu analysieren. Für eine Analyse der Aufzeichnung können Sie eine oder mehrere Stationspaare auswählen. Erfolgt keine Auswahl, werden alle aufgezeichneten Stationspaare analysiert. Die Auswahl der Stationspaare kann in der Spalte *Sel* vorgenommen werden. Die Analyse der Telegramme wird gestartet mit der Schaltfläche **[Analyse]**.

Mit der Funktion [Drucken] wird die Aufzeichnung auf einen Drucker ausgegeben.

Spaltenbeschriftung:

Sel	in der Spalte <i>Sel</i> kann ein Stationspaar nach der Aufzeichnung selektiert werden
Station A	Ethernetadresse der Zielstation zu der nach Beginn der Aufzeichnung zuerst gesendet wurde
Station B	Ethernetadresse der Quellstation die nach Beginn der Aufzeichnung zuerst gesendet hat
Typ	Art des Protokolls (siehe Übersicht Protokolle auf Seite 16)
Frame A->B	Anzahl der Frames die von Station A nach Station B gesendet wurden
Frame A<-B	Anzahl der Frames die von Station B nach Station A gesendet wurden
Byte A->B	Anzahl der Bytes aller Frames die von Station A nach Station B gesendet wurden.
Byte A<-B	Anzahl der Bytes aller Frames die von Station B nach Station A gesendet wurden

Statistik:

Pairs	Anzahl der gefunden Paare während der Aufzeichnung
Frames	Anzahl der aufgezeichneten und ausgewerteten Frames

Kbytes	Die Größe aller Frames in Kbyte
Used	Belegung des Aufzeichnungsspeichers in Prozent
Bdcast	Anzahl an aufgetretenen Broadcast-Telegrammen
FPS	Frames pro Sekunde
Peak	Spitzenwert Frames pro Sekunde
Buffer	Anzahl der empfangenen Frames
<u>Schaltflächen:</u>	
Start	Start der Aufzeichnung
Löschen	Löschen einer Aufzeichnung
Analyse	Analyse einer Aufzeichnung
Drucken	Drucken der aufgezeichneten Stationen

Telegramme aufzeichnen

Über die Schaltfläche [Start] wird die Aufzeichnungsliste gelöscht und eine Aufzeichnung begonnen. Die Schaltfläche [Start] enthält als Indikator eine Led-Anzeige, die anzeigt, ob der Netzwerkanalyzer aufzeichnet. Die Telegramme gelangen von der Netzwerkkarte in den Aufzeichnungspuffer und werden in der Aufzeichnungsliste angezeigt.

Aufzeichnung Stoppen

Die Aufzeichnung wird durch Betätigung der Schaltfläche [Stop] angehalten. Es ist erforderlich, die Aufzeichnung zu stoppen:

- zur Analyse der Aufzeichnung
- zur Sicherung der Analysedaten
- zur Änderung von Parametern und Aktivierung von Filtern

Aufzeichnung Löschen

Die Aufzeichnung wird mit der Schaltfläche [Löschen] gelöscht. Zu jedem beliebigen Zeitpunkt kann der Aufzeichnungspuffer geleert werden. Dies geschieht ohne vorherige Rückfrage.

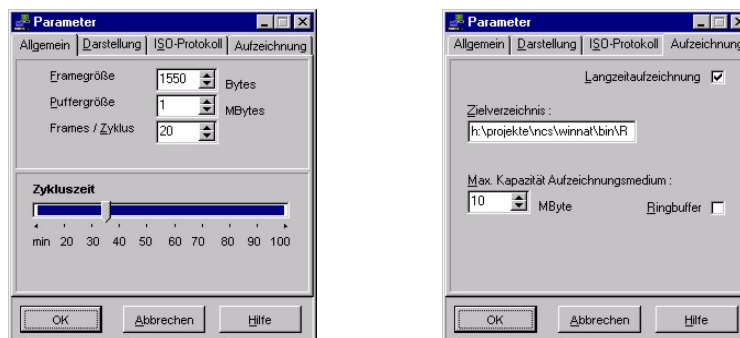
Vor einem erneuten Start wird eine alte Aufzeichnung immer gelöscht.

Langzeitaufzeichnung

Sie aktivieren die Langzeitaufzeichnung indem Sie unter **Analyzer** > *Parameter* im Register "Aufzeichnung" die "Langzeitaufzeichnung" anwählen. In diesem Register können Sie auch ein Zielverzeichnis angeben, in dem Ihre Aufzeichnungsdaten abgelegt werden sollen. Ansonsten werden die Daten wenn der Puffer voll ist, im Verzeichnis "WinNAT\Rec" als Record0.rec, Record1.rec, Record2.rec ... fortlaufend abgelegt.

Die Dateigröße einer einzelnen Record-Datei entspricht dabei den Angaben die Sie zur "Puffergröße" unter **Analyzer**>*Parameter* im Register "Allgemein" vorgenommen haben.

Beachten Sie insbesondere die unter *Parameter Aufzeichnung* einzustellenden Parameter.



Sie starten die Langzeitaufzeichnung aus dem Aufzeichnungsfenster mit [Start]. Es werden wie bei der normalen Aufzeichnung alle Stationspaare im Aufzeichnungsfenster ausgegeben. Sobald Sie [Stop] betätigen, wird die Langzeitaufzeichnung beendet. Durch Klicken auf [Analyse] öffnet sich ein weiteres Aufzeichnungsfenster mit einer Liste der Langzeitaufzeichnungsdateien:

Sel	Frames	Start	Ende	Aufzeichnungsname
	676	13:24:02	13:30:12	Record0.rec
>	415	13:30:13	13:33:43	Record1.rec

Sobald Sie eine Datei auswählen und auf [Laden] klicken, öffnet sich das Analysefenster und die Telegramme der gewünschten Aufzeichnung werden angezeigt.

Spaltenbeschriftung

Sel	in der Spalte <i>Sel</i> kann eine Capturedatei zur Analyse selektiert werden
Frames	Anzahl der Frames in der Capturedatei
Start	Beginn der Aufzeichnung in dieser Capturedatei
Ende	Ende der Aufzeichnung in dieser Capturedatei
Aufzeichnungsname	Fortlaufender Name der Capturedatei bei der Langzeitaufzeichnung

Schaltflächen:

Laden	Die Analyse-Daten der Datei, die Sie selektiert haben, werden geladen und im Analysefenster aufgelistet. Es kann immer nur eine Datei geladen werden.
--------------	---

Analyse

Die Analyse setzt voraus, daß zuvor eine Aufzeichnung stattgefunden hat. Eine bereits durchgeführte Analyse kann auch in einer Datei gesichert bzw. von einer Datei geladen werden.

	Source	Destination	Time-Stamp	Länge	Typ	Parameter
1	080006010011	080006030003	13:35:22.293	60	ISO TP AK	D= 1536 YR-TU-Nr= 29433 CD
2	0020D58202E2	0020D5820282	13:35:22.303	224	TCP	SP= 1033 DP= 139 ACK/
3	0020D58202E2	0020D5820282	13:35:22.303	224	TCP	SP= 1033 DP= 139 ACK/
4	0020D58202E2	0020D5820282	13:35:22.303	224	TCP	SP= 1033 DP= 139 PSH/ACK/
5	0020D5820282	0020D58202E2	13:35:22.303	60	TCP	SP= 139 DP= 1033 ACK/
6	0020D5820282	0020D58202E2	13:35:22.303	105	TCP	SP= 139 DP= 1033 PSH/ACK/
7	0020D58202E2	0020D5820282	13:35:22.313	118	TCP	SP= 1033 DP= 139 PSH/ACK/
8	0020D5820282	0020D58202E2	13:35:22.313	224	TCP	SP= 139 DP= 1033 ACK/
9	0020D5820282	0020D58202E2	13:35:22.313	224	TCP	SP= 139 DP= 1033 ACK/
10	0020D5820282	0020D58202E2	13:35:22.313	224	TCP	SP= 139 DP= 1033 PSH/ACK/
11	0020D58202E2	0020D5820282	13:35:22.313	60	TCP	SP= 1033 DP= 139 ACK/
12	080006010011	080006030003	13:35:22.313	60	ISO TP DT	D= 1536 EOT= End Of TSDU T
13	080006030003	080006010011	13:35:22.313	60	ISO TP AK	D= 1536 YR-TU-Nr= 29433 CD
14	080006030003	080006010011	13:35:22.323	60	ISO TP AK	D= 1536 YR-TU-Nr= 29433 CD
15	080006010011	080006030003	13:35:22.323	60	ISO TP AK	D= 1536 YR-TU-Nr= 29433 CD
16	0020D58202E2	0020D5820282	13:35:22.323	224	TCP	SP= 1033 DP= 139 ACK/
17	0020D58202E2	0020D5820282	13:35:22.323	224	TCP	SP= 1033 DP= 139 ACK/
18	0020D58202E2	0020D5820282	13:35:22.323	224	TCP	SP= 1033 DP= 139 PSH/ACK/

Buttons: Detail, Laden, Sichern, Drucken, Schließen, Hilfe

Für detaillierte Informationen über ein Telegramm klicken Sie auf [Detail]. Es öffnet sich das Detailfenster in dem das ausgewählte Telegramm in seine logischen Bestandteile zerlegt und die einzelnen Schichten des Telegramms angezeigt werden.

Spaltenbeschriftung

Source	Quellstation von der das Telegramm gesendet wurde
Destination	Zielstation die das Telegramm empfangen hat
Time-Stamp	Zeitstempel
Länge	Länge des Telegramms
Typ	Typ des Protokolls (kann sich auch bei einem Stationspaar ändern)
Parameter	die wichtigsten Parameter sind: TP4: (D=Destination-Reference, YR-TU=nächste TPDU-Nr, CDT=Credit) TCP/UDP/ARP/RARP: (SP=Source-Port, DP=Destination-Port und Flags)

Schaltflächen:

Detail	detaillierte Analyse eines Telegramms
Laden	Laden einer zuvor gesicherten Datei mit Analysedaten
Sichern	Sichern von Analysedaten in einer Datei
Drucken	Drucken der analysierten Telegrammdateien

Analyse von Telegrammen

Alle im Analysefenster angezeigten Telegramme werden in der Reihenfolge Ihres Auftretens gelistet. Im Gegensatz zur Aufzeichnungsliste können Sie hier ermitteln, welche Station wann Daten schickt bzw. empfängt. Weiter werden Telegrammlänge und eventuelle Parameter der Telegramme aufgelistet.

Alle Protokolltypen werden erfaßt und angezeigt.

Zur Zeit werden folgende Protokolle analysiert; die Analysen weiterer Protokolle sind in Vorbereitung:

- **ISO-TP4 (H1)** Transport TP4, ARP, RARP, IP (TCP, UDP)
- **TCP/IP 802.2** ARP, RARP, IP (TCP, UDP)
- **TCP/IP Ethernet** ARP, RARP, IP (TCP, UDP)

802.2 – ISO TP4:

Transport-TP4-Telegramme besitzen einen der folgenden TPDU-Typen. Diese dienen zum Verbindungsaufbau, zur Flußkontrolle oder zum eigentlichen Transport der Daten.

ISO TP4 Telegramme werden dem Layer 4 des ISO/OSI-Schichtmodells zugeordnet.

CR (Connect Request)	Zum Aufbau der Verbindung
DR (Disconnect Request)	Wird von der Station gesendet, zur Aufhebung der Verbindung
CC (Connect Confirm)	Wird von der Station zurückgesendet, die CR empfangen hat
DC (Disconnect Confirm)	Wird von der Station gesendet, die DR empfangen hat
AK (Acknowleges)	Dient zur Flußkontrolle und bestätigt den korrekten Daten-Empfang
EA (Expedited Acknowleges)	Dient zur Flußkontrolle und bestätigt den korrekten Eildaten-Empfang
DT (Data)	Damit werden die eigentlichen Nutzdaten gesendet
ED (Expedited Data)	Mit dieser TPDU werden Eildaten gesendet
RJ (Reject)	Zur Wiederholungsanforderung bei Verlust von Telegrammen
ER (Error)	Telegramm mit Grund der Zurückweisung
DG (Datagramm)	Datagrammdienst

TCP/IP 802.2 oder nach Ethernet :

Zu den TCP/IP-Telegrammen gehören u.a. TCP, UDP, ARP und RARP. Diese Telegramme werden dem Layer 3 und 4 des ISO/OSI bzw. TCP/IP-Schichtmodells zugeordnet.

TCP (Transmission-Control-Protocol)

UDP (User-Datagramm-Protocol)

ARP (Adress Resolution Protocol)

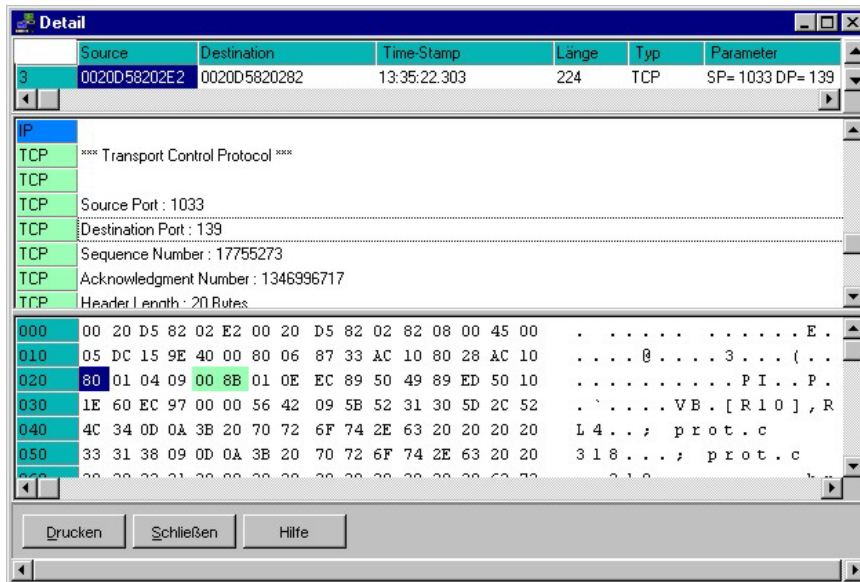
RARP (Reverse Address Resolution Protocol)

NETWARE, NETBEUI, NETBIOS Diese Telegramme werden zur Zeit nicht weiter analysiert.

Detailanalyse

Sie können im Analysefenster ein einzelnes Telegramm aus der Telegrammliste auswählen. Durch Betätigung der Schaltfläche [Detail] öffnet sich das "Detail"-Fenster in dem das Telegramm in seine logischen Bestandteile zerlegt wird und die einzelnen Schichten des Telegramms angezeigt werden.

Hierbei wird eine direkte Beziehung zwischen dem Telegramminhalt in hexadezimaler Form und deren Bedeutung in Klartext hergestellt.



← Telegramm aus Analysefenster

← Telegramminhalt mit Layer-Analyse

← Telegramminhalt in Hex- und ASCII-Darstellung

Das Dialogfenster besteht aus 3 Bereichen:

Telegramm aus Analysefenster

In diesem Bereich des Fensters können sie die Telegrammliste durchblättern.

Telegramminhalt mit Layer-Analyse

In diesem Bereich wird die Bedeutung der einzelnen Telegrammfragmente ausgegeben. Jedes erkannte Fragment eines Telegramms wird in einer separaten Zeile beschrieben. Sie finden schnell über die Zeilenposition des Cursors die Bedeutungen der einzelnen Bytes im Telegramm wieder, da diese im direkten Bezug zur Hexadezimalanzeige angezeigt werden. Die einzelnen Layer eines Telegramms werden farblich unterschieden und mit einer zum Layer passenden Bezeichnung am Beginn jeder Zeile beschriftet.

- *MAC* Layer 1 Media Access Control
- *DLC/LLC* Layer 2 Datalink Control-Header / Local Control/Header
- *ISO CLNP* Layer 3 Connectionless Network Protocol
- *ISO TP* Layer 4 Transport Layer Protocol
- *ISO SESS* Layer 5 Connection-oriented Session Protocol
- *ISO API* Layer 7 S5 AP-Header, TF, FMS

Bei Telegrammen, die nicht weiter analysiert werden, erfolgt nur die Ausgabe der *MAC*- Ebene.

Telegramm in der Hexadezimalanzeige

In diesem Abschnitt werden alle Telegrammartentypen hexadezimal angezeigt. Die einzelnen Telegrammfragmente werden in Bezug zum Klartext farblich unterschiedlich angezeigt.

Parameter

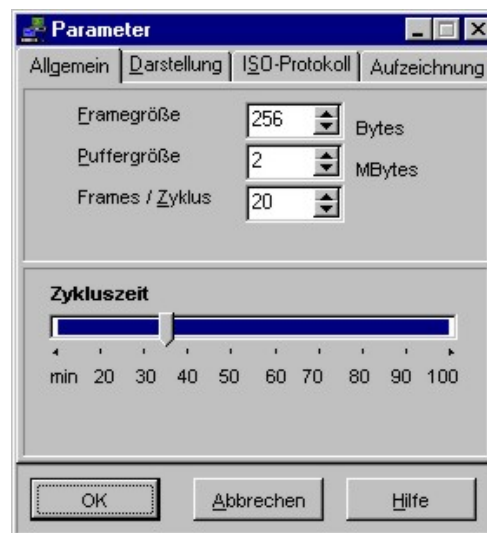
Unter Parameter können Sie verschiedene Einstellungen an WinNAT vornehmen. Die Parameter sind über das Hauptmenü über **Analyzer** > *Parameter* oder in den WinNAT-Fenstern über die rechte Maustaste erreichbar.

Zur Zeit stehen Ihnen folgende Parameter in 4 Registern zur Verfügung:

- **Allgemein** (Parameter für die Aufzeichnung)
- **Darstellung** (Anzeigeformat für Zeit und Adresse)
- **ISO-Protokoll** (TPDU-Format einstellen)
- **Aufzeichnung** (Parameter für die Langzeitaufzeichnung)

Allgemein

In diesem Register können Sie allgemeine Einstellungen zur Aufzeichnung und zur lokalen Rechner-Auslastung vornehmen.



Framegröße	maximale Telegrammgröße in Bytes, die aufgezeichnet wird.
Puffergröße	Größe des Aufzeichnungsspeichers in Megabyte
Frames/Zyklus	Maximale Anzahl an Frames, die pro Zyklus aus der Treiberschicht abgenommen werden.
Zykluszeit	Dauer eines Zyklus in Millisekunden. Damit bestimmen Sie wie häufig die Abnahme von Telegrammdateien, die vom NAT-Treiber bereitgestellt werden, stattfindet. Ist diese Zeit hoch eingestellt, müssen pro Zyklus mehr Daten abgenommen werden (maximal siehe <i>Frames/Zyklus</i>).



Der NAT-Treiber fordert aufgrund der eingestellten Puffergröße einen ebenso großen nicht auslagerungsfähigen Datenbereich an.

Darstellung

Die Darstellung bezieht sich auf die Ausgabe der Adressen und des Zeitstempels im Analysefenster.



Adressanzeige

Telegramme vom Typ TCP/IP können mit Ihrer Ethernetadresse oder IP-Adresse ausgegeben werden. Angezeigt wird die IP-Adresse jedoch erst bei der Telegrammanalyse und nicht bereits bei der Aufzeichnung.

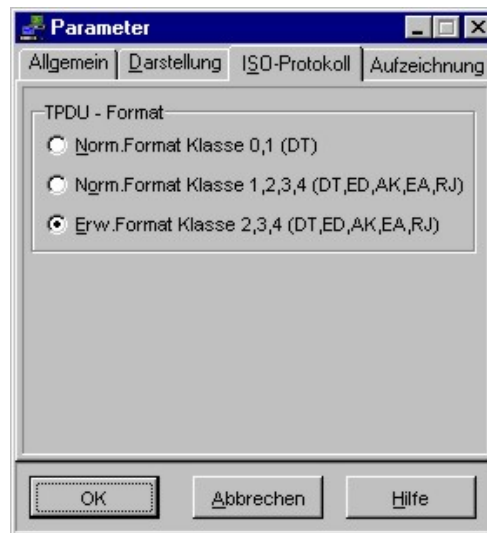
Zeitdarstellung

Zur Zeit wird nur eine absolute Zeitdarstellung unterstützt.
Andere Darstellungsarten sind in Vorbereitung.

ISO-Protokoll

Für ein ISO-TP4 (H1)-Telegramm sind verschieden TPDU-Formate bekannt, die sich in die *normale* und in die *erweiterte* Klasse einteilen lassen. Zusätzlich werden Klassen noch durch Nummernreihen unterschieden.

Welches Format ein TP4-Telegramm tatsächlich besitzt, kann nur bei einem Verbindungsaufbau festgestellt werden. Da der Verbindungsaufbau aber nicht immer aufgezeichnet vorliegt, ist das Format unbestimmt. Sie können jedoch davon ausgehen, dass TP4 (H1)-Telegramme von einer CP immer das "Erweiterte Format Klasse 2, 3, 4" (voreingestellt) besitzen.



TPDU-Format

Über diese Auswahl bestimmen Sie die Interpretation des TPDU-Formats. Voreingestellt ist die Interpretation des Erweiterten Formats für Klasse 2,3,4... .

Aufzeichnung

Unter Aufzeichnung tragen Sie Parameter für die Langzeitaufzeichnung ein.

**Zielverzeichnis**

Hier tragen Sie den Pfadnamen für die Ablage der Capturedateien ein, der für die Langzeitaufzeichnung benutzt wird.

Max. Kapazität

Geben Sie die maximale Kapazität an, die Sie für Ihre Langzeitaufzeichnung zur Verfügung stellen möchten.

Ringbuffer

Bestimmen Sie, ob die Langzeitaufzeichnung in einem Ringbuffer bestehend aus Capturedateien erfolgen soll oder bis zur Grenze der Aufzeichnungskapazität.

Filter

Die Filterfunktionen rufen Sie über das Hauptmenü **Analyzer** > *Filter* oder im Fenster über die rechte Maustaste auf.

In den Filter-Registern können Sie Filterbedingungen für die Aufzeichnung und für die nachfolgende Analyse setzen.

Ein Aufzeichnungsfiler (Hardwarefilter) verhindert, dass bestimmte Telegramme in den Aufzeichnungsspeicher gelangen, während ein Anzeigefiler (Softwarefilter) aus den aufgezeichneten Telegrammen eine entsprechende Selektion trifft. Durch Deaktivierung werden bei einer erneuten Analyse wieder alle Telegramme angezeigt.

Auf jeder Dialogseite befindet sich der Schalter *Filter aktiv*, der für die aktuelle Seite die Filterfunktion ein- oder ausschaltet.

Zu Ihrer Information über den Status der Filter wird bei aktiviertem Hardwarefilter im Aufzeichnungsfenster "Hardwarefilter aktiv" und bei einem aktivierten Softwarefilter im Analysefenster "Softwarefilter aktiv" eingeblendet.

Stationen (Hardwarefilter)

Bei dem Filter *Stationen* handelt es sich um einen Aufzeichnungsfiler. Geben Sie hier immer 12-stellige Ethernet-Adressen an.

Nur die Stationen von Liste A bzw. Liste B werden aufgezeichnet. Je maximal 10 Stationen können in der Liste aufgenommen werden.



Zur Eingabe einer Stationsadresse wählen Sie ein Listenelement aus und geben Sie die Ethernetadresse ein. Bei aktivierter Symbolik können Sie aus dem Auswahlfeld einen symbolischen Namen aussuchen, der dann in die Liste übernommen wird.

Zum Löschen wählen Sie ein Element aus der Liste aus und drücken Sie die Entf.-Taste.

Richtung

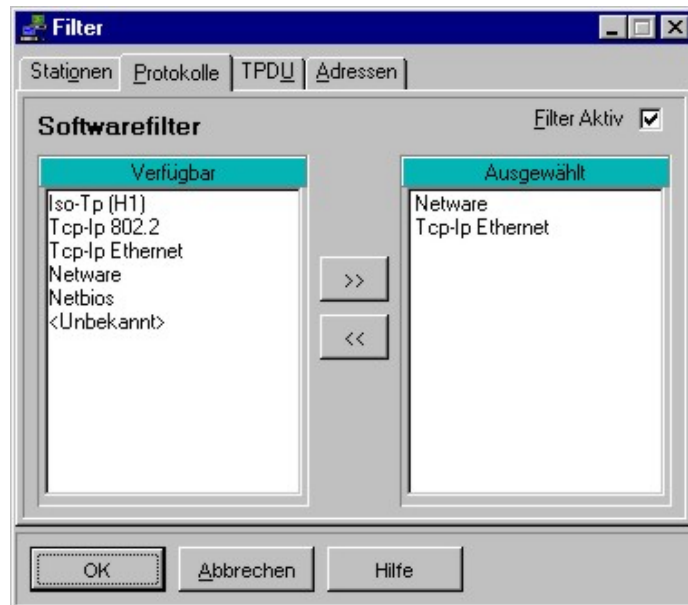
bestimmt die Aufzeichnungsrichtung für alle Einträge in der Liste

Jede Station

Sie können entweder gewünschte Stationsadressen in eine Liste eintragen oder Sie wählen "Jede Station" an. Dies entspricht dem Eintrag aller Stationen in der neben stehenden Liste.

Protokolle (Softwarefilter)

Bei dem Filter *Protokolle* handelt es sich um einen Anzeigefilter zur Protokollselektion.



Ein oder mehrere Protokolle können aus der Liste der verfügbaren Protokolle in die Liste der ausgewählten Protokolle aufgenommen werden. Die Übernahme und die Rücknahme von Einträgen tätigen Sie durch Markieren der entsprechenden Listeneinträge und anschließendem Drücken der Schaltfläche Übernahme [>>] bzw. Rücknahme [<<].

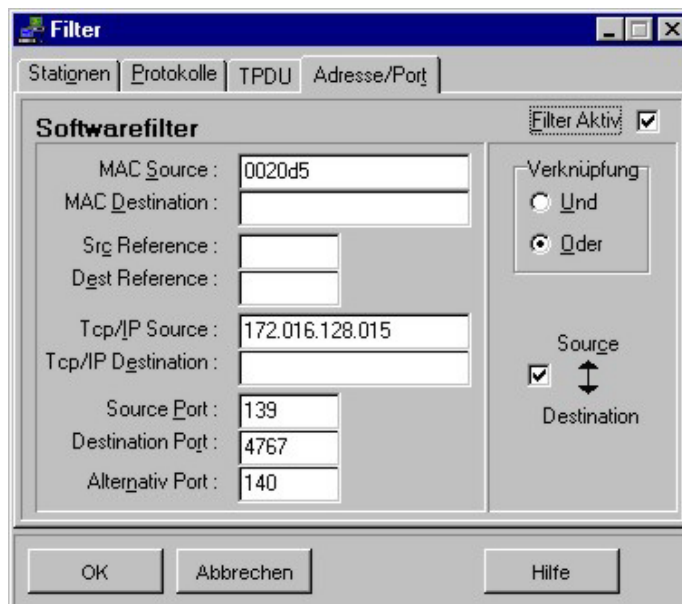
TPDU (Softwarefilter)

Bei dem Filter *TPDU* handelt es sich um einen Anzeigefilter zur TPDU-Selektion von H1-Telegrammen. Ein oder mehrere TPDU-Typen können ausgewählt werden.



Adressen (Softwarefilter)

Bei dem Filter *Adressen/Ports* handelt es sich um einen Anzeigefilter zur Selektion von Telegrammen in Bezug auf Adresse und Port. Nur Telegramme, deren Adressen und Ports den Angaben entsprechen, werden zur Anzeige gebracht.



MAC- Source/Destination

Tragen Sie in Source bzw. Destination die gewünschte Ethernetadresse (MAC-Adresse) ein.

Geben Sie als Adresse einen unvollständigen Wert an, wird auf dieses Fragment gefiltert.

Src/Dest Reference

Die Source- bzw, Destination-Referenzen sind Zahlenwerte, die dem entsprechenden TSAP zugeordnet sind. Sie werden beim Verbindungsaufbau zwischen den Stationen festgelegt.

TCP/IP- Source/Destination

Tragen Sie in Source bzw. Destination eine IP-Adresse ein.

Source/Destination/ Alternative Port

Port entspricht der Port-Nr. einer TCP/IP-Verbindung. Unter *Alternative Port* können Sie eine zusätzliche Port-Nr. angeben, die ersatzweise für Source/Destination Port Anwendung findet.



Sobald Sie diese Funktion aktivieren, werden die Richtungen (Source und Destination) ignoriert.

Verknüpfung Und/Oder

Mit *Und* stellen Sie ein, dass nur Telegramme angezeigt werden, die alle angegebenen Bedingungen erfüllen. Bei *Oder* muss mindestens eine der Bedingungen erfüllt sein.

Symbol-Manager

Symbolische Adressierung

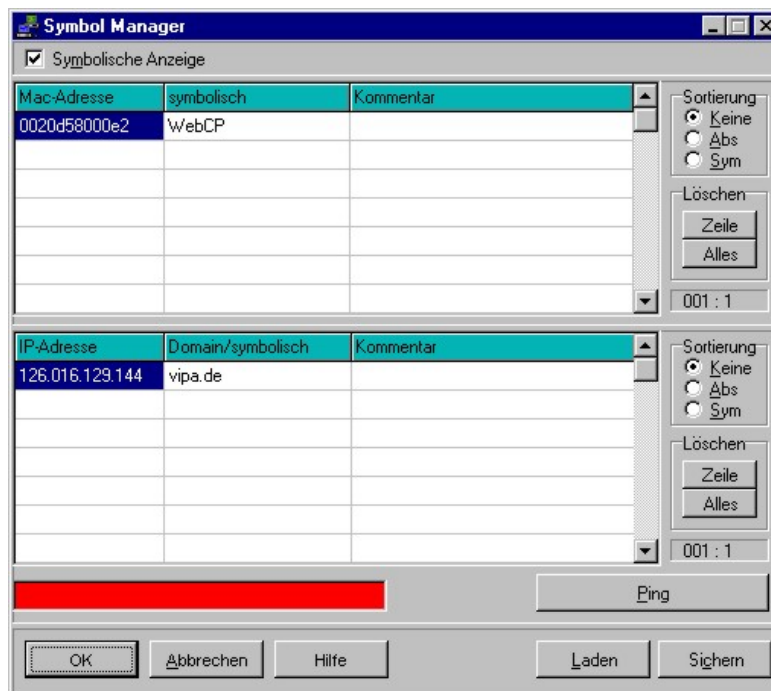
Die symbolische Adressierung gibt Ihnen die Möglichkeit den Ethernetadressen und IP-Adressen symbolische Namen zuzuweisen. Konventionen zur Vergabe eines Namens bestehen nicht. Die einzige Restriktion besteht in der Länge der Namen. Die Namen sollten aus nicht mehr als 20 Zeichen bestehen, da diese an verschiedenen Stellen ab dem zwanzigsten Zeichen abgeschnitten werden.

Haben Sie die symbolische Adressierung eingeschaltet, erscheinen überall im Programm die symbolisch vergebenen Namen, an denen sonst die absolute Adresse erscheint. Die symbolischen Namen stehen Ihnen auch bei Auswahl-Eingabefeldern zu Verfügung.

Doppelt vergebene Namen für Ethernetadressen bzw. IP-Adressen werden bei einer Übersetzung festgestellt und angezeigt. Zur besseren Übersichtlichkeit kann eine Sortierung nach *absoluter* Adresse oder nach *symbolischem* Namen vorgenommen werden. Keine Sortierung erfolgt unter *keine*.

Funktionen des Symbolmanagers

Die einzelnen Funktionen werden im folgenden detailliert beschrieben:



Symbolische Anzeige

Ist *Symbolische Anzeige* abgehakt, erscheinen in allen Programmteilen die den absoluten Adressen zugewiesenen symbolischen Adressen. Der Kommentar erscheint nur in der Symbolverwaltung.

Sortierung

Sie können im Symbolmanager über *absolut* bzw. *symbolisch* sortieren oder die Sortierung über *keine* abschalten.

Schaltflächen:

OK

Nach Betätigung der Schaltfläche [OK] werden die Listen geprüft und es erscheint ein Hinweisfenster falls ungültige bzw. doppelt vergebene symbolische Namen vorkommen. Bei [Abbruch] gehen alle Änderungen verloren.

Laden, Sichern

Bei einem neuen Programmstart wird immer die letzte aktuelle Symbolliste geladen. Bei verschiedenen Anlagen ist es jedoch sinnvoll die Symbollisten als Datei abzulegen. Eine erstellte Symbolliste kann über die Schaltfläche [Sichern] in einer Datei gesichert werden bzw. eine zuvor gesicherte Datei über die Schaltfläche [Laden] in die Symbolverwaltung geladen werden.

Ping

Mit der Ping-Funktion können Sie ermitteln, ob die Zielbaugruppe physikalisch im Netz vorhanden ist.

Positionieren Sie hierzu den Fokus auf die gewünschte IP-Adresse in der Symboltabelle.

Mit einem Ping wird eine ICMP-Message an die Zielbaugruppe gesendet. Daraufhin schickt die Baugruppe innerhalb einer gewissen Reaktionszeit eine Antwort zurück. Das Ergebnis erscheint als Textausgabe.

War Ping erfolgreich, wird die Meldung "Ping-Echo" in n ms ausgegeben, ansonsten wird eine Fehlermeldung angezeigt.

Alles löschen

Klicken Sie auf [Alles] werden nach einer Sicherheitsabfrage alle Einträge gelöscht.

Zeile löschen

Mit Strg-Entf können Sie die Zeile löschen, in der Sie sich gerade befinden.

Zeile einfügen

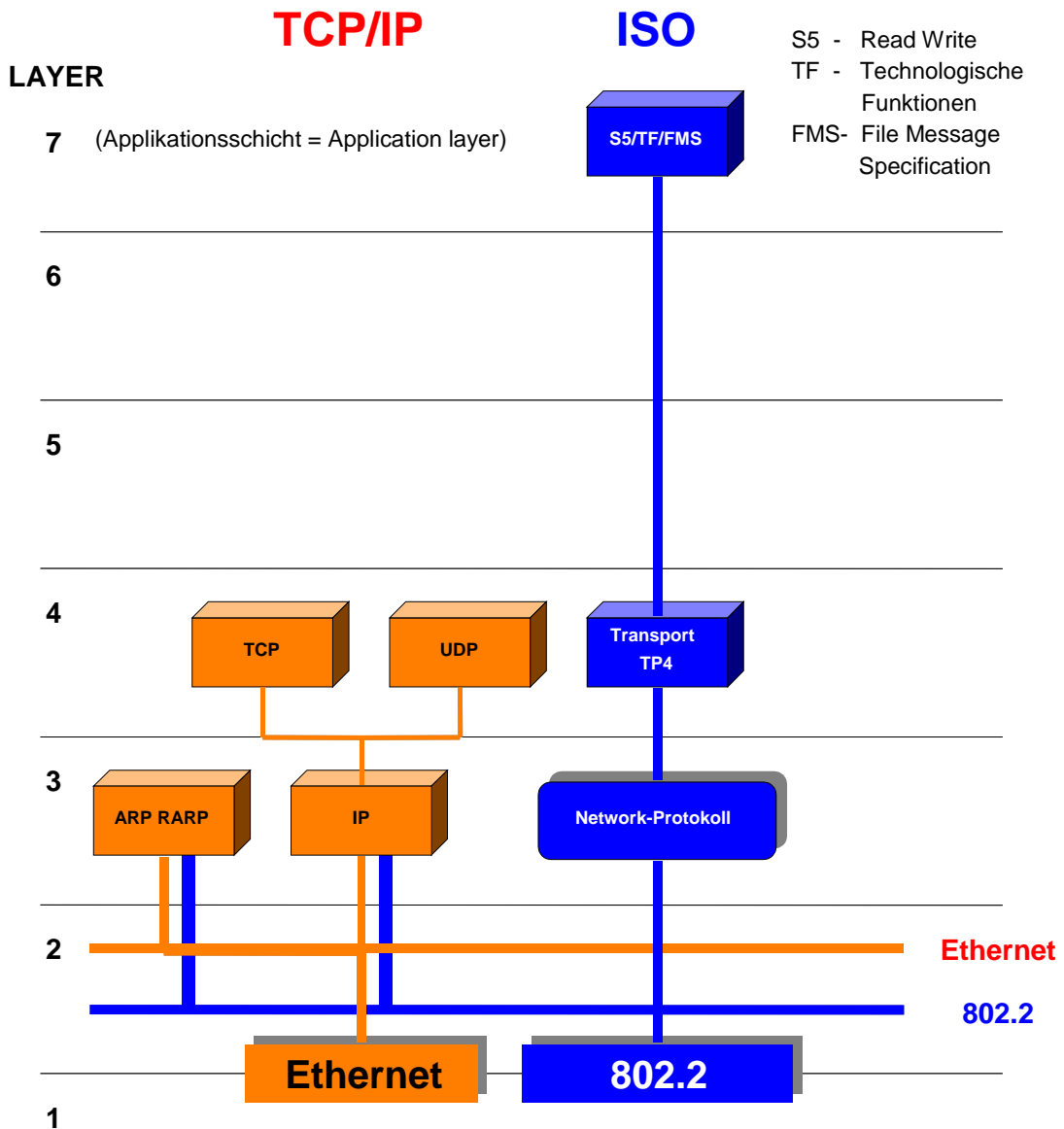
Mit Strg-Einf fügen Sie oberhalb der aktuellen Markierung ein leere Zeile ein.

Die Zahlenangaben am unteren Rand der beiden Listen informieren über die aktuelle Cursoposition *Zeile* : *Spalte*. Die Angaben finden Sie auch in den Fehlermeldungen.

Übersicht Protokolle

Alle Protokolltypen werden erfaßt und angezeigt. Eine Analyse erfolgt zur Zeit jedoch nur über die folgenden Protokolle:

- Ethernet-TCP/IP** ARP, RARP, IP (TCP, UDP)
- 802.2 – ISO** Transport TP4, ARP, RARP, IP (TCP, UDP)



Glossar

AP

Applikations Protokoll

AG

Automatisierungs-Gerät

BCD

Binary-Coded Decimal (binär codierte Dezimalzahl)

CP

Communication-Processor (H1 und TCP/IP)

DNS

Domain Name System

GSD

Gerätestammdatei

HTB

Hantierungsbaustein

IP

Internet Protocol

IPK

Intelligente Prozeßkommunikation

ISO

International Organisation for Standardization

LAN

Local Area Network

Layer

Schicht im ISO/OSI-Schicht-Modell (1 bis 7)

MMS

Manufacturing Message Specification

NAT

Network Analyzer Treiber

OSI

Open Systems Interconnection

PDU

Process Data Unit

QVZ

Quittungsverzug

SNMP

Simple Network Management Protocol

TCP

Transport Control Protocol

TP

Transport-Protokoll

TPDU

Transport Protocol Data Unit

TRADA

Transparenter Datenaustausch

TSAP

Transport Service Access Point

UDP

User Datagram Protocol

BDE

Database Engine, zur Verwaltung der Datenbank

Index

A

Analyse 16
 von Telegrammen 17
Aufzeichnung 8, 14
Aufzeichnungsfenster 13

D

Detailanalyse 18
Druckerausgabe 9
Druckoptionen 9

F

Filter 23

I

Installation des Treibers 5

L

Langzeitaufzeichnung 15
Lieferumfang 3

N

Netzwerk einrichten 5
Netzwerkanalyzer 10
 Arbeitsweise 11

P

Parameter 19
Ping 27
Protokolle 17
 Übersicht 28

S

Symbolische Adressierung 26
Symbol-Manager 8
Systemanforderungen 3

W

WinNAT
 beenden 6
 Hauptfenster 8
 Hilfefenster 7
 Installation 4
 Kontextmenü 7
 Menüleiste 8
 Registrierung 4
 starten 6
 Struktur 12
 Verzeichnisstruktur 6

