

LPA / LPA-IP™

LOYTEC Protokollanalysator

Benutzerhandbuch

LOYTEC electronics GmbH

The screenshot displays the 'Active Log Running' window of the LOYTEC protocol analyzer. It features a table of network packets and a detailed view of the selected packet (Packet Number 3).

Number	Time	Length	Flags	TX#	Domain	Source	Destination	Service	Data
1	15:18:42.795000	12	-- -- --	5	--	01/09	01/07	ACKD	UPDT[0005] 04
2	15:19:04.607000	9	-- -- --	5	--	01/07	01/09	ACK	
3	15:19:43.654000	15	-- -- --	5	112233	03/01	#01	UnACKD_RPT	UPDT[0006] 11 22
4	15:19:45.201000	15	-- -- --	5	112233	03/01	#01	UnACKD_RPT	UPDT[0006] 11 22
5	15:19:45.873000	15	-- -- --	5	112233	03/01	#01	UnACKD_RPT	UPDT[0006] 11 22
6	15:20:58.092000	16	-- --	-	--	00/00	*/*	UnACKD	NETMGMT[Service Pin] 01 00 17 81 70

General Packet Information
Packet Number: 3
Time: 2006/01/10 15:19:43.654000
Length: 15 DataLength: 2
TX Number: 5 CRC: 8C2D
Service: Repeated (UnACKD)

Flags
 Priority
 Alternate Path
 Authenticated
 Idempotent

Address and Message Information
Domain: 112233
Source: S/N: 03/01
Destination: Group: 01
Message: Network Variable Update

Update [0006] to 11 22

Packet Structure:
PREAMBLE LENGTH: 16
PPDU HEADER (LINK/MAC PROTOCOL DATA UNIT)
MPDU HEADER (NETWORK PROTOCOL DATA UNIT)
01 [00-----] Protocol Version 0
01 [--00----] TransportPDU included
01 [----01--] Address Format 1 (Group)
01 [-----10] Domain Length 3 Bytes
Source Subnet/Node 03/01 (003/001)
Destination Group 01 (001)
Domain 11 22 33
TPDU HEADER (TRANSPORT PROTOCOL DATA UNIT)
01 [0-----] Non-Authenticated Packet
01 [-001----] TPDU Type 1 (Unacknowledged Repeated Service)
01 [-----0101] Transaction Number 05 (005)
APDU (APPLICATION PROTOCOL DATA UNIT)
Network Variable Update, Selector 0006 (00006)
Data0000: 11 22
CRC 8C2D

0000: 00 06 03 81 01 11 22 33 15 80 06 11 22 2D 8C

Kontakt

LOYTEC electronics GmbH
Blumengasse 35
1170 Wien
ÖSTERREICH
support@loytec.com
<http://www.loytec.com>

Version 3.7

Dokument Nr. 88063218

LOYTEC GIBT KEINE UND SIE ERHALTEN KEINE GARANTIEN ODER ABMACHUNGEN, WEDER AUSGESPROCHEN, NOCH UNAUSGESPROCHEN, WEDER SATZUNGSGEMÄSS NOCH IN IRGEND EINER KOMMUNIKATION MIT IHNEN, UND LOYTEC LEHNT JEDLICHEN ANSPRUCH AUF UNAUSGE-SPROCHENE GARANTIEN BEZÜGLICH DER GEBRAUCHSTAUGLICHKEIT ODER TAUGLICHKEIT FÜR IRGEND EINEN BESTIMMTEN GEBRAUCH AB. DIESES PRODUKT IST NICHT DAFÜR KONZIPIERT, IN EINER AUSTRÜSTUNG FÜR CHIRURGISCHE IMPLANTATE IM KÖRPER VERWENDET ZU WERDEN, NOCH IST ES DAFÜR KONZIPIERT, IN ANDEREN ANWENDUNGEN, DIE LE-BEN UNTERSTÜTZEN ODER ERHALTEN, IN DER FLUGKONTROLLE ODER MASCHINENKONTROLLE INNERHALB DER AUSTRÜSTUNG VON FLUG-ZEUGEN ODER IRGEND EINER ANDEREN ANWENDUNG VERWENDET ZU WERDEN, IN WELCHER FEHLER DIESES PRODUKTES ZU EINER SITUATION FÜHREN KÖNNEN, IN WELCHER PERSONEN VERLETZT WERDEN ODER DEREN TOD EINTRETEN KÖNNTE.

LOYTEC ÜBERNIMMT KEINERLEI GARANTIEN FÜR DIE IN DIESEM DOKUMENT GELISTETEN PRODUKTE VON DRITTANBIETERN.

Ohne vorherige schriftliche Einwilligung von LOYTEC darf kein Teil dieser Veröffentlichung kopiert oder nachgebildet, in einem Abfragesystem gespeichert, in irgend einer Form oder mit irgendwelchen Mitteln, elektronisch, mechanisch, fotokopiert, aufgenommen oder in irgendeiner anderen Form übermittelt werden.

LC3020™, L-Chip™, L-Core™, L-DALI™, L-GATE™, L-INX™, L-IOB™, L-IP™, LPA™, L-Proxy™, L-Switch™, L-Term™, L-VIS™, L-WEB™ und ORION™ Stack sind Markennamen von LOYTEC electronics GmbH.

LonTalk®, LonWorks®, Neuron®, LonMark®, LonMaker®, i.LON® und LNS® sind Markennamen von Echelon Corporation, die in den USA und anderen Staaten registriert wurden.

Inhalt

1	Einführung	5
2	Installation und Konfiguration.....	6
2.1	Soft- und Hardware-Installation.....	6
2.2	Netzwerk-Interface Konfiguration und Produktregistrierung.....	6
2.3	Netzwerk-Interface- und Transceiver-Auswahl	7
2.3.1	NIC709-PP, NIC709-USB und NIC709-PCI Geräte	7
2.3.2	NIC852-Geräte (LPA-IP).....	8
2.3.3	Remote-LPA Geräte.....	10
2.3.4	NIC-IP Geräte	13
2.3.5	Multiplexed Network Interfaces (MNI-Geräte).....	13
2.4	Datei Öffnen mittels Kommandozeile	15
2.5	LPA-Konfigurationen	15
2.6	Gleichzeitige Verwendung mehrerer LPAs.....	15
2.7	Server-Modus	16
3	Tutorial	17
4	Verwendung des LPAs	21
4.1	LPA Menüs	21
4.2	Werkzeugleiste.....	22
4.3	Logfenster	24
4.4	Statusleiste.....	26
4.5	Suchen und Anspringen von Paketen	27
4.6	Funktionen des Kontextmenüs (View-Menüs)	28
4.7	Paketaufzeichnung vom Netzwerk.....	29
4.8	Logdateien.....	29
4.9	Exportieren einer Logdatei.....	30
4.10	Drucken einer Logdatei.....	30
4.11	Hilfdatei	31
5	Erweiterte Funktionen des LPAs	32
5.1	Logmodus	32
5.2	Paketkonverter	33
5.3	Paketfilter und -trigger	36
5.4	Anzeigeoptionen.....	41
5.5	Paketstatistik.....	42
5.6	Knotenstatistik.....	44
5.7	LPA-Reports	47

5.8	Statistiktrend	48
5.9	Paketsimulation	49
5.10	Packet-Recording-Dateien	51
5.11	LPA-Einstellungen	52
6	Externe Applikationen	55
6.1	Datenverarbeitung von Packet-Recording-Dateien.....	55
6.2	LPA-Server und -Clients.....	55
6.3	LPA-Plug-Ins	57
6.4	LPA Report-DLLs.....	59
7	Versionsverzeichnis.....	61
	Abkürzungen.....	63
	Abbildungsverzeichnis	64
	Index	66

1 Einführung

Der LOYTEC Protokollanalysator (LPA) ist ein vielseitiges Werkzeug zur Analyse von CEA709 und CEA852 / CNIP (Control Network over IP) Netzwerken mittels eines LOYTEC NIC709 oder NIC852 Netzwerk-Interfaces, welches Ihren PC mit dem Netzwerk verbindet. Nach Konfiguration des LPA kann der gesamte Datenverkehr geloggt und online angezeigt werden. Durch die zahlreichen Filter-, Konvertierungs- und Statistikfunktionen können Sie mit dem LPA alle gerade interessanten Informationen extrahieren. Mittels der LPA-IP und Remote-LPA Funktionen kann auf beliebige CEA852 und CEA709 Netzwerke von jedem Punkt der Welt aus über das Internet zugegriffen werden. Außerdem arbeitet die LPA-Software auch problemlos mit externen Applikationen zusammen, siehe Kapitel 6. Für Software-Updates und weitere aktuelle Informationen - den LPA sowie andere LOYTEC Produkte betreffend - besuchen Sie bitte unsere Homepage (<http://www.loytec.com>).

Im ersten Teil des Benutzerhandbuchs wird kurz auf die Installation und Konfiguration des LPAs eingegangen. Es folgt ein kurzes Tutorial, um den Einstieg zu erleichtern. Danach werden schließlich alle grundlegenden und erweiterten Funktionen des LPAs beschrieben. Bitte beachten Sie, dass mit dem Ausdruck „LPA Software“ sowohl die LPA-SW als auch die LPA-IP-SW Software bezeichnet wird.

2 Installation und Konfiguration

2.1 Soft- und Hardware-Installation

Um die Installation zu starten, legen Sie bitte die LOYTEC Software CD in Ihr CDR/DVD-Laufwerk. Falls das CD-Menü nicht automatisch erscheint, starten Sie bitte die Datei „setup.exe“. Installieren Sie zunächst das NIC-Softwarepaket durch Anklicken des entsprechenden Menüpunkts. Danach lesen Sie bitte das NIC Benutzerhandbuch, welches sich in Ihrem NIC Installationsverzeichnis (z.B. „C:\Programme\LOYTEC\NIC“) unter ‚Doc\German‘ befindet. Es enthält eine detaillierte Beschreibung des Installations- und Konfigurationsvorgangs Ihres NIC709 bzw. NIC852 Netzwerk-Interfaces.

Als nächsten Schritt installieren Sie bitte die LPA Software. Klicken Sie wieder auf den entsprechenden Menüpunkt im LOYTEC CD-Menü und folgen Sie den Anweisungen. Informationen zur Konfiguration Ihrer Personal Firewall finden Sie im NIC Benutzerhandbuch.

2.2 Netzwerk-Interface Konfiguration und Produktregistrierung

Um Ihr LOYTEC Netzwerk-Interface zu konfigurieren, starten Sie das LOYTEC Konfigurations-Tool („LConfig“) aus Ihrem Windows Startmenü (in „LOYTEC Network Interfaces“). Eine genaue Beschreibung des Konfigurationsvorgangs finden Sie im NIC Benutzerhandbuch sowie der Online-Hilfe des LConfig-Tools.

Um Ihre LPA Software zu registrieren, wählen Sie [Menü Help | Register Product...] im LPA und geben Sie im Dialog (siehe Abbildung 1) den Registrierungscode ein, welcher Ihrem LPA Paket beigelegt ist.

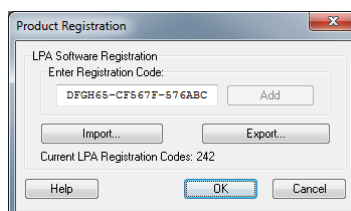


Abbildung 1: LPA Software-Registrierung

Klicken Sie anschließend auf "Add" und dann auf "OK". Wollen Sie mehrere LPA Lizenzen (für verschiedene Netzwerk-Interfaces) registrieren, geben Sie die Registrierungscode, wie gerade beschrieben, der Reihe nach ein. Bereits eingegebene Registrierungscode können exportiert und bei weiteren Softwareinstallationen importiert werden.

2.3 Netzwerk-Interface- und Transceiver-Auswahl

Wenn Sie die LPA Software zum ersten Mal starten, müssen Sie zunächst Ihr Netzwerk-Interface sowie einen aktiven Transceiver auswählen. Um ein Netzwerk-Interface auszuwählen, klicken Sie auf **NI** oder wählen Sie [Menü Profile | Network Interface...]. Alle installierten Netzwerk-Interfaces werden nun angezeigt, siehe Abbildung 2.

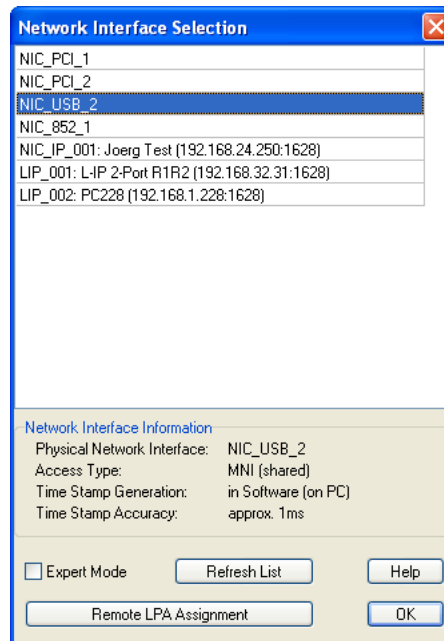


Abbildung 2: Netzwerk-Interface Auswahl

Sollte ein installiertes Netzwerk-Interface nicht aufscheinen, starten Sie bitte das LConfig-Tool und testen Sie das entsprechende Netzwerk-Interface. Wenn ein bestimmtes Netzwerk-Interface nicht verfügbar ist ("Device not available"), so wird es bereits von einer anderen Anwendung benutzt. Wenn Sie auf ein Netzwerk-Interface klicken, erscheinen im unteren Bereich des Fensters weiterführende Informationen, siehe dazu auch Abschnitt 2.3.5. Wählen Sie Ihr Netzwerk-Interface durch Doppelklick in die entsprechende Zeile oder durch Klick auf "OK". Sie können die Liste der Netzwerk-Interfaces neu einlesen, indem Sie auf "Refresh List" klicken. Weiters besteht die Möglichkeit, zwischen Standard- und Expert-Mode für "Multiplexed Network Interfaces" (siehe Abschnitt 2.3.5) zu wechseln, sowie Remote-LPA Geräte (siehe 2.3.3) zuzuweisen.

Nach Auswahl des Netzwerk-Interfaces muss noch mittels [Menü Profile | Interface Settings...] oder Anklicken von **IF** ein Transceiver ausgewählt werden. Das entsprechende Dialogfenster sowie weitere Details der verschiedenen Netzwerk-Interface-Typen sind in den folgenden Abschnitten beschrieben.

2.3.1 NIC709-PP, NIC709-USB und NIC709-PCI Geräte

Dieser Abschnitt deckt sowohl die NIC709 Netzwerk-Interface-Serie (ausgenommen NIC709-IP) sowie ältere Typen, wie "LPA006", "LPA-PP" und "LPA-USB" ab. Diese Netzwerk-Interfaces werden verwendet, um einen PC direkt mit einem CEA709 Netzwerk zu verbinden. Abbildung 3 zeigt beispielhaft den entsprechenden Aufbau bei einem NIC709-USB.

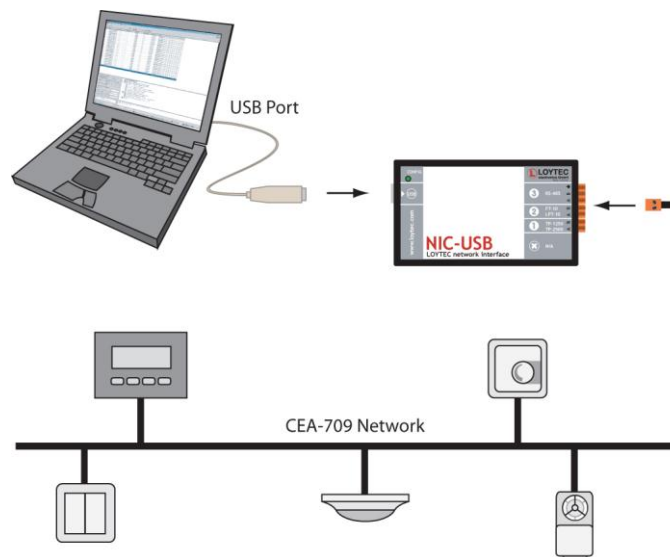


Abbildung 3: NIC709-Aufbau

Das CEA709-Netzwerk muss mit dem passenden Transceiver des NIC709 Netzwerk-Interfaces verbunden werden. Der Transceiver muss dann im "Interface Settings"-Dialog der LPA Software ausgewählt werden. Abbildung 4 zeigt das entsprechende Dialogfenster für NIC709 Netzwerk-Interfaces.

Für jeden der drei Ports kann ein Transceiver gewählt werden. Die zugehörige Bitrate wird daneben angezeigt. Es muss außerdem ein bestimmter Port aktiviert werden, mittels Anklicken einer der drei kleinen Knöpfe auf der linken Seite. Durch Anklicken von "Test" kann überprüft werden, ob das Netzwerk-Interface korrekt funktioniert. Beim RS-485-Transceiver (Port 3) können Sie außerdem versuchen, die Bitrate automatisch zu detektieren. Nach Klick auf "Detect" wird das Netzwerk bei unterschiedlichen Bitraten untersucht. Die korrekte Bitrate kann allerdings nur detektiert werden, wenn während der Detektierung Pakete empfangen werden.

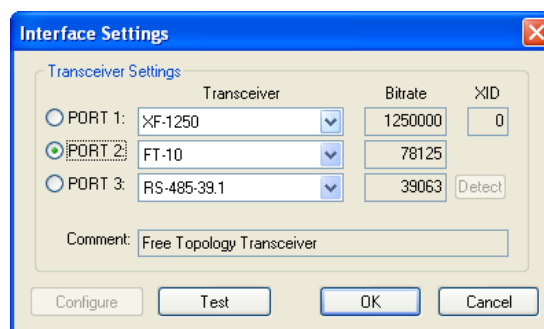


Abbildung 4: NIC709 Transceiver-Auswahl

2.3.2 NIC852-Geräte (LPA-IP)

Beim Erwerb eines LPA-IP Pakets, erhalten Sie einen NIC852 USB-Key, um Ihrem PC die Verbindung zu einem CEA852 / CNIP (Control Network over IP) Netzwerk zu ermöglichen. Alternativ ist auch ein software-aktiviertes NIC852-SW-Produkt erhältlich. Der Standardanwendungsfall für NIC852 ist, als Teilnehmer (Knoten) am CEA852 / CNIP Kanal (LonMark IP-852) zu fungieren, siehe Abbildung 5.

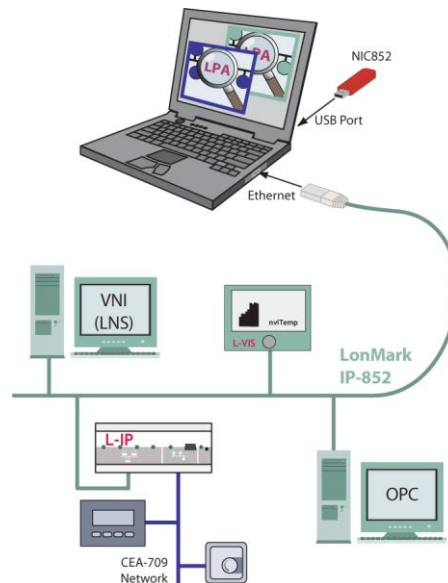


Abbildung 5: LPA-IP auf NIC852

In diesem Fall empfängt die LPA-IP-SW Software den gesamten Verkehr des IP-852 Kanals. Im NIC Benutzerhandbuch ist beschrieben, wie ein NIC852 konfiguriert werden muss, um Teilnehmer eines CEA852 Kanals zu werden. Bitte beachten Sie, dass aufgrund der Punkt-zu-Punkt Charakteristik von CEA852 Ungenauigkeiten in der Paketaufzeichnung entstehen können. Abbildung 6 zeigt den Grund dieses Verhaltens.

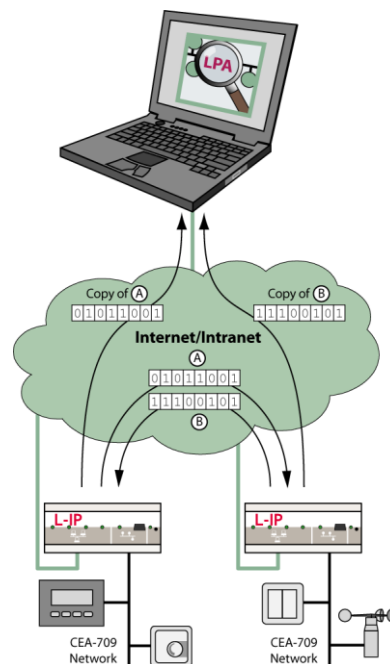


Abbildung 6: Paketaufzeichnung auf CEA852

Wenn ein LPA in einen bestehenden CEA852 Kanal eingefügt wird, schicken die restlichen Kanalteilnehmer automatisch *Kopien* aller ausgesendeten Pakete an den LPA. In Abbildung 6 z.B. sendet der linke L-IP das Paket A an den rechten L-IP und eine Kopie des Pakets A an den LPA. Der rechte L-IP sendet das Paket B an den linken L-IP und eine Kopie des Pakets B an den LPA. Daher ist es möglich, dass die Paketreihenfolge für einige Transaktionen im LPA Logfenster falsch angezeigt wird (z.B. kann eine "Response" vor dem "Request" <A> angezeigt werden). Außerdem besteht die Möglichkeit, dass die Kopie des Pakets im LPA sichtbar ist, das Originalpaket jedoch

- sein Ziel nicht erreicht hat,
- im Empfänger verworfen wurde, aufgrund eines falsch eingestellten Channel-Timeouts
- oder aufgrund einer unsynchronisierten Uhr,

und vice versa. Dies kann vor allem in WANs (Wide Area Networks) vorkommen, wo die Paketübertragungszeit von unterschiedlichen Knoten sehr verschieden sein kann, und Pakete auch verloren gehen können. Weiters ist auch die Genauigkeit der Zeitstempel, welche im LPA angezeigt werden, stark von der IP-Paketübertragungsdauer abhängig. In LANs (Local Area Networks) hingegen sollten diese Effekte nur minimal in Erscheinung treten.

Abbildung 7 zeigt das "Interface Settings" Dialogfenster der LPA Software für NIC852. Hier können Sie lediglich zwischen IP-10L (LAN) und IP-10W (WAN) wählen.

Ein weiterer Anwendungsfall für NIC852 ist die direkte Verbindung mit einem Remote-LPA Gerät sowie das Aufzeichnen von Paketen vom CEA709-Port des Geräts, siehe Abschnitt 2.3.3.

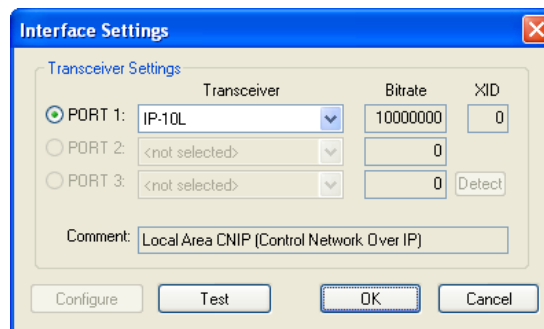


Abbildung 7: NIC852 Transceiver-Auswahl

2.3.3 Remote-LPA Geräte

Die LPA-IP-SW Software in Kombination mit einem NIC852 kann dazu verwendet werden, den Verkehr des CEA709-Ports eines Geräts mit Remote-LPA Funktion (z.B. LOYTEC L-IP-Router) aufzuzeichnen. In diesem Anwendungsfall muss der PC nicht notwendigerweise ein Teilnehmer des entsprechenden CEA852 Kanals sein. Vielmehr wird der LPA-IP Punkt-zu-Punkt über das Internet/Intranet mit dem entsprechenden Gerät (z.B. L-IP) verbunden.

Im Beispiel von Abbildung 8 werden zwei LPA Logs gestartet, auf jedem L-IP ein Log. Jedes LPA Logfenster zeigt dabei den lokalen Verkehr am CEA709-Port des entsprechenden L-IPs. Um Remote-LPA Geräte zu suchen und der LPA-IP-SW Software zuzuweisen, wird ein "Remote Device Discovery and Assignment"-Modul verwendet, welches durch Anklicken von "Remote LPA Assignment" im "Network Interface" Dialogfenster (siehe Abbildung 2) gestartet wird. Abbildung 9 zeigt das "Remote LPA Assignment" Dialogfenster.

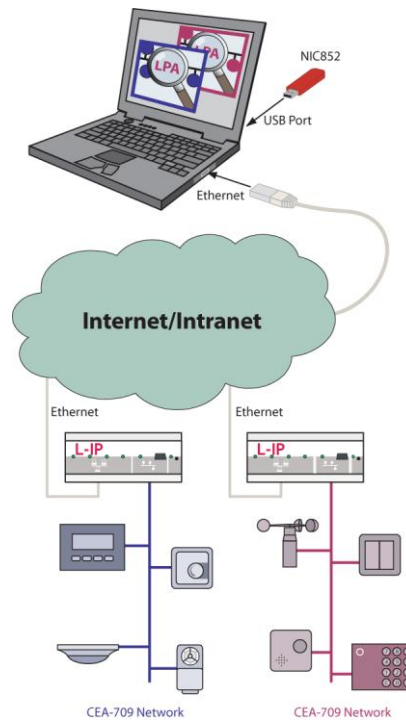


Abbildung 8: Remote-LPA auf L-IP

In der Gerätetabelle werden alle gefundenen Geräte angezeigt. Alle Geräte ohne Remote-LPA Funktion bzw. Geräte, die nicht erreicht werden können, werden grau dargestellt. Mittels "Show All Devices" kann entschieden werden, ob alle Geräte oder nur Remote-LPA Geräte angezeigt werden sollen. Während der Gerätesuche können bereits gefundene Geräte zugewiesen werden. Es ist also nicht nötig, das Ende der Suche abzuwarten, da dies in großen Netzen sehr lange dauern kann.

No.	S	Assignment	IP/NAT Address	Port	Device Type	Device Name	Interface	Config. Server	Location
1		LIP_001	192.168.1.254	1628	L-IP	<noname>	Port 1	<unknown>	unknown
2		LIP_002	90.18.145.23	1628	L-IP	alexander	EIA709	21.47.75.1	unknown
3		LIP_003	62.78.15.77	1628	L-IP	chris	EIA709	21.47.75.1	unknown
4		LIP_004	62.78.95.196	1628	L-IP	thomas	EIA709	21.47.75.1	unknown
5		LIP_005	80.8.23.71	1628	L-IP	dietmar	EIA709	21.47.75.1	unknown
6		LIP_006	62.40.48.2	1628	L-IP	hans-joerg	EIA709	21.47.75.1	Brunnkirchen
7		LIP_007	192.168.1.228	1628	L-IP	axls_cs	EIA709	192.168.1.228	unknown
8		LIP_008	192.168.1.229	1628	L-IP	axls_cc	EIA709	192.168.1.228	unknown
9		LIP_009	192.168.1.209	1628	L-IP	local	EIA709	192.168.1.209	unknown
10		LIP_010	192.168.32.4	1628	L-IP	lip3	EIA709	192.168.1.209	unknown
11			192.168.12.5	1628	NIC-IP	Alexander2	EIA709	<unknown>	Alexander's Desk
12			192.168.24.250	1628	NIC-IP	<noname>	EIA709	<unknown>	unknown
13			192.168.12.4	1628	NIC-IP	<no_response>	<unknown>	<unknown>	<no_response>
14			192.168.17.126	1628	NIC-IP	BMUZ_84	EIA709	<unknown>	Backbone BMUZ 84
15			192.168.32.11	1628	NIC-IP	lip3	EIA709	<unknown>	unknown
16			192.168.1.59	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
17			21.47.75.1	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
18			80.8.21.36	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
19			192.168.1.96	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
20			192.168.1.39	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
21			192.168.1.40	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>
22			192.168.1.140	1628	<no_response>	<no_response>	<unknown>	<unknown>	<no_response>

Show All Devices

Device Discovery

15 Devices Found. Finished Remote Device Discovery Process.

Abbildung 9: Remote LPA Assignment

Um ein Remote-LPA Gerät zuzuweisen, wählen sie die entsprechende Zeile in der Gerätetabelle und klicken Sie auf "Assign/Add" oder doppelklicken Sie auf das zuzuweisende Gerät. Um ein Gerät hinzuzufügen, welches sich nicht in der Tabelle befindet, klicken Sie ebenfalls auf "Assign/Add". Das entsprechende Dialogfenster ist in Abbildung 10 dargestellt.

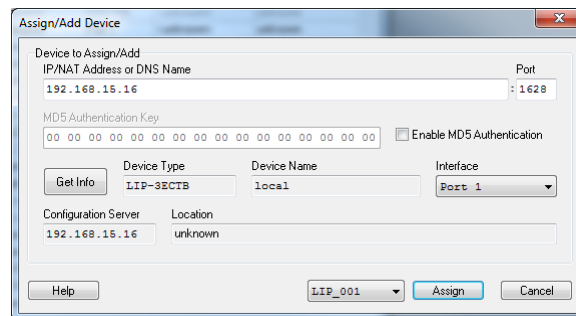


Abbildung 10: Zuweisen/Hinzufügen eines Remote-LPA Geräts

Die IP-Adresse sowie der Port können manuell in den Feldern " IP/NAT Address or DNS Name" und "Port" eingestellt werden. Sollte sich das Gerät hinter einem NAT-Router befinden, so müssen Sie hier die Adresse des NAT-Routers eintragen. Sie können auch einen DNS Namen statt der IP Adresse eintragen. Sollte MD5 im Gerät eingeschaltet sein, so muss "Enable MD5 Authentication" aktiviert und der korrekte "MD5 Authentication Key" eingetragen werden. In diesem Fall zeigt ein kleines Schlüsselsymbol in der Assignment-Spalte der Gerätetabelle die aktivierte Authentifizierung an, siehe Abbildung 9. Bevor Sie das Gerät zuweisen, können Sie noch auf "Get Info" klicken, um den Gerätenamen ("Device Name"), den Gerätetyp ("Device Type"), die Interface-Liste ("Interface"), den Configuration-Server sowie den Ort ("Location") zu überprüfen. Schließlich wählen Sie ein logisches Gerät (LIP_001 ... LIP_512) und klicken auf "Assign", um das Gerät zuzuweisen.

Um automatisch alle verfügbaren Geräte zuzuweisen, klicken Sie auf "Auto Assign" im Remote-LPA Assignment Fenster (Abbildung 9). Sie können die Geräteliste zuvor sortieren, indem Sie auf einen bestimmten Spaltenkopf klicken. Gerätezuweisungen können mittels der Knöpfe "Clear", "Clear All", "Load" und "Save" gelöscht, geladen und gespeichert werden. Sollten keine Geräte gefunden werden oder wollen Sie einen weiteren CEA852-Kanal hinzufügen, so klicken Sie bitte auf "Add Device". Es erscheint das in Abbildung 11 gezeigte Dialogfenster.

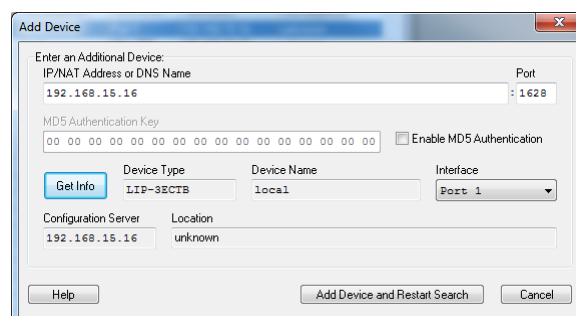


Abbildung 11: Hinzufügen eines CEA852-Kanals

Ähnlich dem "Assign/Add"-Dialog können Sie hier die IP/NAT-Adresse oder den DNS Namen, die Portnummer und optional den MD5-Key eines Teilnehmers des gewünschten CEA852-Kanals eingeben. Mit "Get Info" können Sie die Erreichbarkeit des Geräts überprüfen. Schließlich klicken Sie auf "Add Device and Restart Search" um den Suchvorgang erneut starten. Alle Teilnehmer des neuen Kanals sollten nun in der

Geräteliste aufscheinen. Beachten Sie, dass Sie mindestens einen Teilnehmer des neuen Kanals zuweisen müssen ("Assign/Add"), um den Kanal permanent zu speichern.

Mittels des "Wink"-Knopfs im Remote-LPA Assignment-Dialog können Sie das gewählte Gerät dazu bringen, mit einigen LEDs zu blinken. Dies kann benutzt werden, um bestimmte Geräte im Feld zu identifizieren. Klicken Sie schließlich auf "OK" um die Zuweisung abzuschließen. Im "Network Interface" Dialogfenster erscheinen die zugewiesenen Geräte als "LIP_001", "LIP_002", usw., siehe Abbildung 2.

Es ist nicht nötig, den Transceiver für Remote-LPA Geräte zu wählen, da dieser durch die physikalische Konfiguration des Geräts festgelegt ist. Wenn Sie allerdings das "Interface Settings"-Dialogfenster aufrufen, so wird der CEA709-Transceiver der gewählten Geräts angezeigt, siehe Abbildung 12. Die angezeigte Port-Nummer ist in diesem Fall lediglich eine Eigenschaft der physikalischen Transceiver-Verbindung am Gerät und kann daher ignoriert werden.

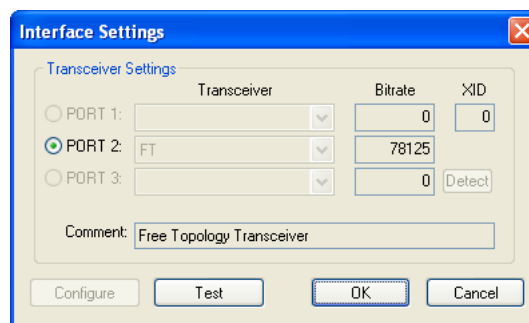


Abbildung 12: Transceiver-Anzeige für Remote-LPA Geräte

Beachten Sie, dass die Zeitstempel, welche im LPA Logfenster angezeigt werden, lokal im Remote-LPA Gerät generiert werden. Sollten die Zeitstempel fehlerhaft sein, so muss die Zeit im Gerät nachjustiert werden. Informationen dazu erhalten Sie in der entsprechenden Gerätedokumentation.

2.3.4 NIC-IP Geräte

Alle Einstellungen für NIC-IP Geräte werden nun im L-Config-Tool vorgenommen, siehe NIC Benutzerhandbuch.

2.3.5 Multiplexed Network Interfaces (MNI-Geräte)

Die NIC-PCI, NIC-USB, NIC-IP und NIC852 Netzwerk-Interfaces können in einem "Multiplexed Network Interface"-Modus betrieben werden. Jedes physikalische Netzwerk-Interface wird dabei durch 8 Multiplexed Network Interfaces (MNI-Geräte) repräsentiert. Das bedeutet, dass Sie bis zu 8 unterschiedliche Applikationen gleichzeitig am selben Netzwerk-Interface betreiben können. Dies "virtuellen Interfaces" verhalten sich wie Knoten auf einem "virtuellen Kanal", welcher über das physikalische Netzwerk-Interface mit dem physikalischen Kanal verbunden ist, siehe Abbildung 13.

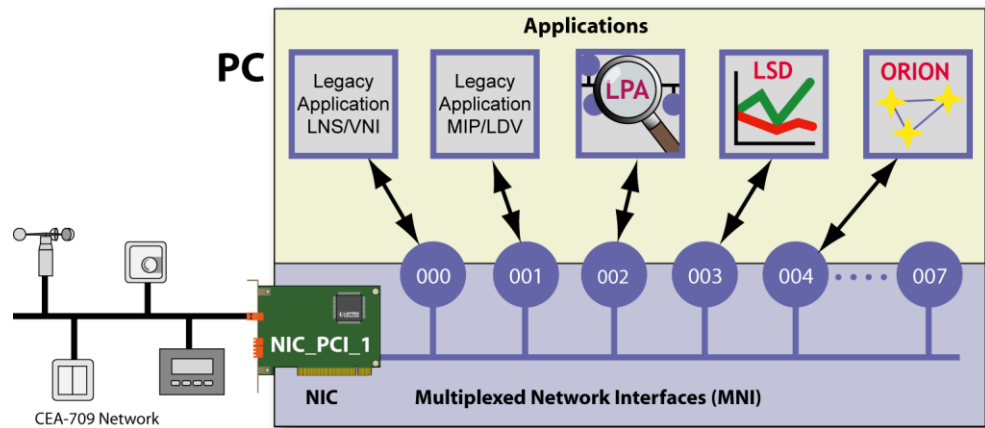


Abbildung 13: Multiplexed Network Interfaces

Sie können z.B. die LPA Software, das LSD Tool, eine weitere ORION-Applikation, eine LNS/VNI Applikation sowie eine MIP/LDV Applikation gleichzeitig auf einem NIC709-PCI Netzwerk-Interface betreiben.

Im Standardmode der Netzwerk-Interface-Auswahl („Expert Mode“ deaktiviert, siehe Abbildung 2) werden, soweit vom Netzwerk-Interface unterstützt, automatisch MNI-Geräte benutzt. Auf diese Weise können z.B. LPA und LSD Software gleichzeitig auf demselben Netzwerk-Interface "NIC_PCI_1" betrieben werden. Im "Expert Mode" werden sowohl das physikalische Interface (z.B. "NIC_PCI_1") als auch alle zugehörigen MNI-Geräte angezeigt ("NIC_PCI_1_000", "NIC_PCI_1_001", "NIC_PCI_1_002", usw.) und können explizit ausgewählt werden, siehe Abbildung 14. Die mit [reserved] markierten Geräte sind für Legacy-Applikationen reserviert und sollten nicht ausgewählt werden.

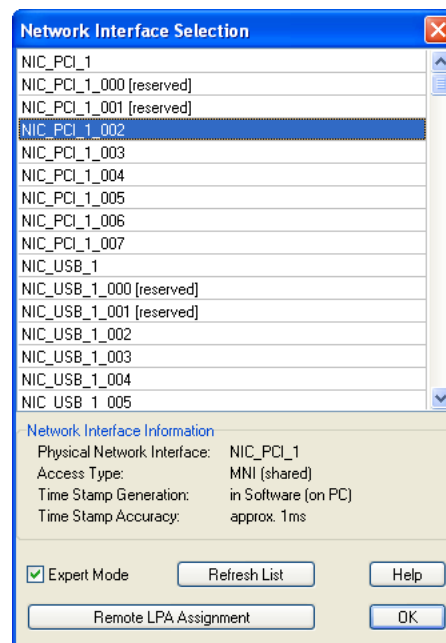


Abbildung 14: Expert Mode bei der Netzwerk-Interface-Auswahl

Es folgt eine Aufstellung der Unterschiede zwischen physikalischen Netzwerk-Interfaces und MNI-Geräten:

- Alle MNI-Geräte erhalten dieselbe Seriennummer (Seriennummer des physikalischen Geräts).

- Sollte das physikalische Netzwerk-Interface bereits verwendet werden, so sind die MNI-Geräte dieses Interfaces nicht mehr verfügbar und vice versa.
- LPA-Zeitstempel werden in Software erzeugt, wenn von einem MNI-Gerät aufgezeichnet wird (im Gegensatz zum physikalischen Netzwerk-Interface, wo die Zeitstempel in der Hardware generiert werden), und haben deshalb eine geringere Genauigkeit.

Der Name des physikalischen Netzwerk-Interfaces, die Zugriffsart (Access Type) sowie Informationen über die Zeitstempelerzeugung werden im unteren Teil des Auswahlfensters eingeblendet, siehe Abbildung 2 und Abbildung 14. Ansonsten verhält sich ein MNI-Gerät exakt wie das entsprechende physikalische Netzwerk-Interface. Für die LPA-Software ist es daher vollkommen transparent, ob das darunter liegende Netzwerk-Interface ein MNI-Gerät ist oder nicht. Bitte beachten Sie, dass der NIC Legacy-Treiber laufen muss, um die MNI-Geräte zu aktivieren.

2.4 Datei Öffnen mittels Kommandozeile

Um eine Paketlogdatei beim Start des LPAs zu öffnen, kann der Kommandozeilenparameter '-f' verwendet werden:

z.B.: 'C:\Programme\LOYTEC\LPA\LPA.exe -f log_name1.plg'

Alternativ dazu kann nach Installation der LPA-Software eine Logdatei auch einfach über Doppelklick im Explorer geöffnet werden.

2.5 LPA-Konfigurationen

Mittels Kommandozeilenparameter ist es möglich, verschiedene LPA-Konfigurationen aufzusetzen. Wenn Sie eine neue LPA-Konfiguration erstellen wollen, so erzeugen Sie zunächst eine neue Verknüpfung zur Datei 'LPA.exe' aus dem LPA-Installationsverzeichnis. Danach wählen Sie per rechter Maustaste die Eigenschaften der Verknüpfung und fügen im Feld 'Ziel' einen eindeutigen Konfigurationsnamen an:

z.B.: 'C:\Programme\LOYTEC\LPA\LPA.exe' ⇒

'C:\Programme\LOYTEC\LPA\LPA.exe KonfigName1'

Der Name des neuen LPA-Symbols sollte ebenfalls entsprechend angepasst werden, um es von anderen Konfigurationen unterscheiden zu können. Die eben beschriebene Prozedur können Sie mit verschiedenen Konfigurationsnamen beliebig oft wiederholen, um mehrere, voneinander unabhängige LPA-Konfigurationen zu erhalten. Alle Einstellungen, die Sie dann in der LPA-Software vornehmen, betreffen nur die jeweilige Konfiguration des LPA-Symbols, das Sie zum Start der Software verwendet haben. Alle anderen Konfigurationen bleiben dabei unverändert.

2.6 Gleichzeitige Verwendung mehrerer LPAs

Wenn Sie mehrere Kanäle gleichzeitig beobachten wollen, können Sie dazu mehrere LPA-Instanzen gleichzeitig verwenden. Starten Sie einfach für jeden Kanal einmal die LPA-Software. Beachten Sie, dass Sie dabei für jede Instanz das korrekte Netzwerk-Interface (siehe Abschnitt 2.3) einstellen müssen. Um zu verhindern, diese Einstellungen bei jedem Start erneut vornehmen zu müssen, können Sie, wie in Abschnitt 2.4 beschrieben, verschiedene LPA-Konfigurationen (eine für jedes Netzwerk-Interface) aufsetzen.

2.7 Server-Modus

Die LPA-Software kann in einem speziellen Server-Modus gestartet werden. Detaillierte Informationen zur LPA-Server-Funktion finden Sie in Abschnitt 6.2. Im Server-Modus startet der LPA automatisch einen Paketlog und leitet alle Pakete (welche das Aufzeichnungsfiler passieren) zu den LPA-Clients weiter. Um den Server-Modus zu aktivieren, muss der LPA mit der Option "-s" gestartet werden. Um die Server-Modus-Konfiguration von der normalen LPA-Konfiguration (bzw. von anderen LPA-Konfigurationen, siehe Abschnitt 2.4) zu unterscheiden, wird empfohlen, dem Server-Modus eine eigene Konfiguration zuzuweisen. Der LPA muss dazu z.B. folgendermaßen gestartet werden:

```
'C:\Programme\LOYTEC\LPA\LPA.exe ServerConfig -s'
```

Eine entsprechende Verknüpfung kann in das Autostart-Verzeichnis des Startmenüs eingetragen werden, um den LPA-Server beim Hochfahren des PCs automatisch zu starten. Da im Server-Modus keine grafische Benutzerschnittstelle verfügbar ist, müssen alle notwendigen Einstellungen (Netzwerk-Interface, Paketkonverter, Aufzeichnungsfiler, usw.) in einem vorangehenden Schritt durchgeführt werden, indem der LPA ohne die Option "-s" jedoch mit dem verwendeten Server-Modus-Konfigurationsnamen gestartet wird:

```
'C:\Programme\LOYTEC\LPA\LPA.exe ServerConfig'
```

Beim Beenden wird die Konfiguration dann automatisch gespeichert. Sobald der LPA im Server-Modus gestartet wird, erscheint ein Systray-Icon, welches den Zustand des LPA-Servers anzeigt, siehe Abbildung 15.



Abbildung 15: LPA-Server Systray-Icon

Die Farbe des Icons zeigt folgende Zustände an:

- Grau ... Inaktiv (Pause) oder auf das Öffnen des Netzwerk-Interface wartend
- Grün ... Aktiv
- Rot ... Ein Fehler ist aufgetreten

Wenn der Mauszeiger auf das Icon zeigt, werden zusätzliche Informationen, den Zustand des LPA-Servers betreffend, angezeigt. Außerdem erscheint durch Rechtsklick ein Menü, siehe Abbildung 16.



Abbildung 16: Systray-Icon Menü

Durch Doppelklick auf das Icon oder Auswahl von 'Pause' im Menü, kann die LPA-Server-Funktion unterbrochen bzw. wieder fortgesetzt werden. Falls ein Fehler beim Hochstarten des LPA-Servers aufgetreten ist, kann mittels 'Start' ein erneuter Startversuch vorgenommen werden. Per 'Exit' wird der LPA-Server beendet.

3 Tutorial

Dieses Tutorial soll den Einstieg in die wichtigsten Funktionen der LPA-Software erleichtern. Eine detaillierte Beschreibung aller Funktionen wird in den Kapiteln 4 und 5 vorgenommen. Die hier beschriebenen Schritte können alle ohne real vorhandenes Netzwerk vorgenommen werden.

1.) Starten Sie den LPA und klicken Sie auf den Knopf .

Sie haben nun ein neues Logfenster zur Anzeige empfangener Pakete erzeugt. Es handelt sich dabei um das sogenannte ‘aktive Logfenster’ (‘Active Log’), siehe Abbildung 17.

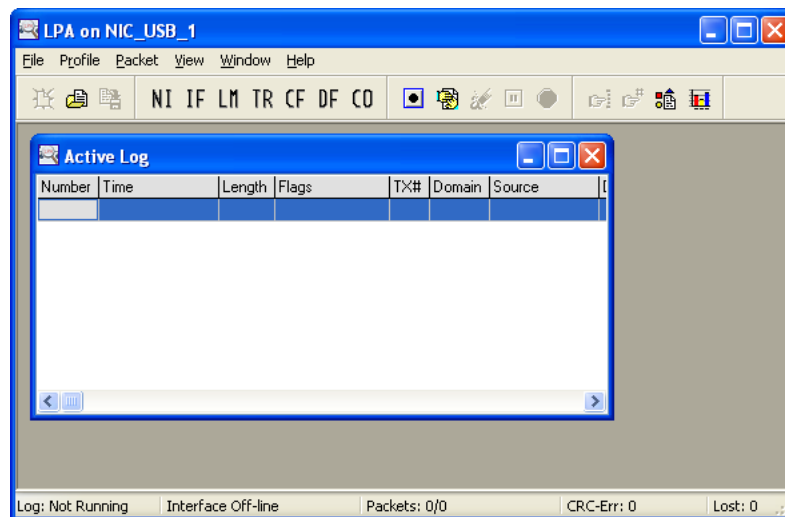



Abbildung 17: Aktives Logfenster

2.) Starten Sie den Logprozess mittels [Menü Packet | Start Log | from File (trace)...].

Es sollen nun Pakete von einer Datei geloggt werden, um ein reales Netzwerk zu simulieren. Ein Dialogfenster erscheint, mit welchem Sie die Datei ‘tutorial.prc’ öffnen. Nun können Sie im Logfenster die eintreffenden Pakete beobachten. Jedes Paket entspricht dabei einer Zeile der Pakettabelle, wie in Abbildung 18 gezeigt wird.

Number	Time	Length	Flags	TX#	Domain	Source	Destination	Service	Data
1	14:06:22.435	12	-- -- ---	0	--	02/02	01/01	ACKD	UPDT [0001] 10
2	14:06:24.435	9	-- -- ---	0	--	01/01	02/02	ACK	
3	14:06:26.435	12	-- -- ---	1	--	02/02	01/01	ACKD	UPDT [0001] 20
4	14:06:28.435	9	-- -- ---	1	--	01/01	02/02	ACK	
5	14:06:30.435	12	-- -- ---	2	--	02/02	01/01	ACKD	UPDT [0001] 30

Abbildung 18: Eintreffende Pakete

3.) Unterbrechen Sie den Logprozess per Klick auf .

4.) Klicken Sie mit der rechten Maustaste in das Logfenster und wählen Sie 'Packet Details'.

Wann immer Sie mit der rechten Maustaste in ein Logfenster klicken, erscheint ein Kontextmenü, welches zur Konfiguration der Paketanzeige benutzt wird. Es werden nun detaillierte Informationen zum gerade ausgewählten Paket angezeigt, siehe Abbildung 19.

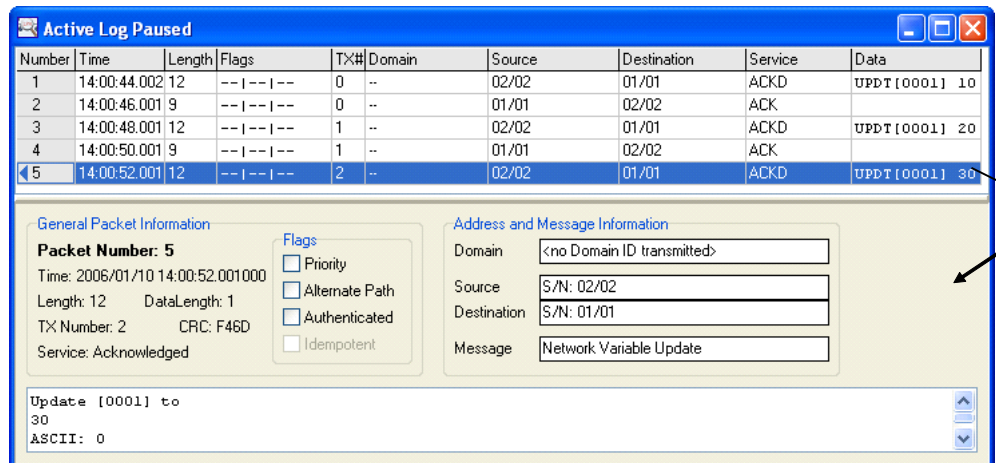


Abbildung 19: **Paketdetails**

5.) Klicken Sie mit der rechten Maustaste in das Logfenster und wählen Sie 'Protocol Details'.

Nun werden zusätzlich alle protokollspezifischen Informationen des Pakets angezeigt (siehe Abschnitt 4.3). Sie können die Paket- und Protokolldetails wieder ausblenden, indem Sie die Schritte 4 und 5 wiederholen.

6.) Editieren Sie den Paketkonverter per Klick auf .

Es erscheint ein Dialogfenster, in welchem Sie auf den Knopf 'Open' klicken und die Datei 'tutorial.pco' öffnen. Der Paketkonverter wird benutzt, um statt der im Paket enthaltenen Nummern (für Adressen und Netzwerkvariablen) symbolische Namen im Logfenster anzeigen zu können. Klicken Sie nun auf 'OK'. Die Darstellung der Spalten 'Domain', 'Source' (Absenderadresse), 'Destination' (Empfängeradresse) und 'Data' des Logfensters wird gemäß den Konvertertabellen verändert, siehe Abbildung 20.

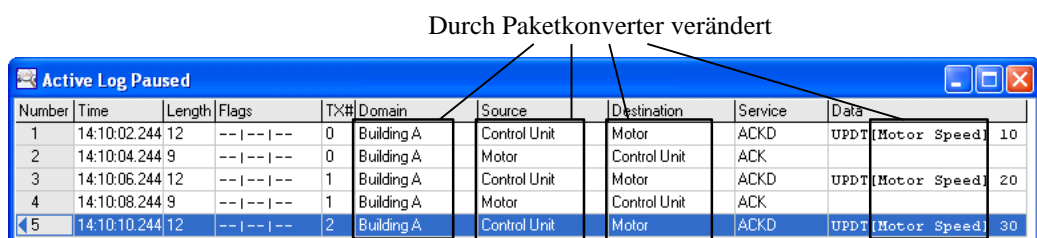




Abbildung 20: **Konvertierte Pakete**


7.) Editieren Sie das Anzeigefilter (Display Filter) per Klick auf .

Das Anzeigefilter entscheidet, welche der geloggtten Pakete angezeigt werden sollen. Standardmäßig können alle Pakete das Filter passieren und werden dem gemäß im Logfenster angezeigt. Um eine Idee von der Arbeitsweise des Filters zu bekommen, aktivieren Sie zunächst den Filter mittels „Enable Display Filter“. Klicken Sie dann auf die ‘Layer 4’-Filtersektion und aktivieren Sie das Feld ‘Enable TPDU Filter’. Nun können Sie Filterparameter auf Schicht 4 des Netzwerkprotokolls konfigurieren. Deaktivieren Sie das Feld ‘Acknowledgements’, um alle Acknowledgements (Bestätigungsnachrichten) auszublenden. Wenn Sie nun auf ‘OK’ klicken, werden die vorgenommenen Änderungen übernommen.

8.) Deaktivieren Sie das Anzeigefilter per Klick auf  und Klick in das Feld ‘Enable Display Filter’.

Nachdem Sie mit ‘OK’ bestätigt haben, werden die versteckten Pakete wieder eingeblendet. Das gesamte Anzeigefilter ist nun deaktiviert und alle empfangenen Pakete werden im Logfenster angezeigt.

Beachten Sie, dass neben dem Anzeigefilter auch ein Aufzeichnungsfiler existiert, welches zuallererst entscheidet, ob empfangene Pakete gespeichert werden sollen, siehe Abschnitt 5.3.

9.) Starten Sie den Logprozess erneut per Klick auf .

10.) Rufen Sie mittels Klick auf  das Paketstatistikfenster auf.

Daraufhin erscheint das in Abbildung 21 dargestellte Fenster. Es zeigt verschiedene Paketstatistikdaten an (siehe Abschnitt 5.5).

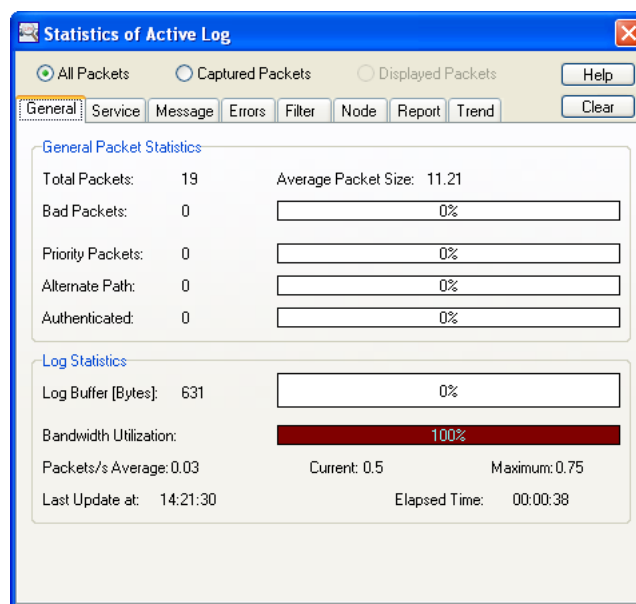



Abbildung 21: Paketstatistikfenster

11.) Warten Sie, bis alle Pakete der Demonstrationsdatei ‘tutorial.prc’ geloggt sind.

Sobald alle Pakete geloggt sind, erscheint die in Abbildung 22 gezeigte Dialog-Box, in welcher Sie auf ‘OK’ klicken. Sie können den Logprozess auch jederzeit manuell durch Klick auf den Knopf  beenden.

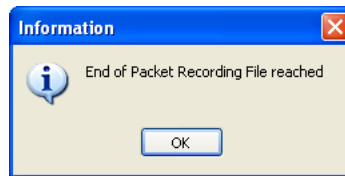



Abbildung 22: Ende der Demonstrationsdatei

12.) *Speichern Sie den Paketlog per Klick auf .*

Es erscheint ein Dialogfenster, wo Sie den Log unter dem Namen 'test.plg' speichern. Danach können Sie das Logfenster mittels [Menü File | Close] schließen. Eine Sicherheitsabfrage nach Speicherung des Anzeigefilters ('Save Changes to Display Filter') können Sie per Klick auf 'No' übergehen.

13.) *Öffnen Sie die eben gespeicherte Logdatei per Klick auf .*


Es erscheint wieder ein Dialogfenster, wo Sie die eben gespeicherte Datei 'test.plg' öffnen. Beachten Sie, dass dadurch auch automatisch die entsprechende Konverterdatei ('tutorial.pco') geöffnet wird. Abbildung 23 zeigt das Logfenster, welches nun erscheinen sollte.

Number	Time	Length	Flags	TX#	Domain	Source	Destination	Service	Data
1	14:10:02.244000	12	-- --- ---	0	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 10
2	14:10:04.244000	9	-- --- ---	0	Building A	Motor	Control Unit	ACK	
3	14:10:06.244000	12	-- --- ---	1	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 20
4	14:10:08.244000	9	-- --- ---	1	Building A	Motor	Control Unit	ACK	
5	14:10:10.244000	12	-- --- ---	2	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 30
6	14:21:03.482000	9	-- --- ---	2	Building A	Motor	Control Unit	ACK	
7	14:21:05.482000	11	-- --- ---	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
8	14:21:07.482000	11	-- --- ---	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
9	14:21:09.482000	11	-- --- ---	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
10	14:21:11.482000	14	-- --- ---	3	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 28
11	14:21:13.482000	10	-- --- ---	3	Building B	Lamp	Control Unit	ACK	
12	14:21:15.482000	14	-- --- ---	4	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 38
13	14:21:17.482000	10	-- --- ---	4	Building B	Lamp	Control Unit	ACK	
14	14:21:19.482000	14	-- --- ---	5	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 48
15	14:21:21.483000	10	-- --- ---	5	Building B	Lamp	Control Unit	ACK	
16	14:21:23.483000	12	-- --- ---	6	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 8C
17	14:21:25.483000	14	-- --- ---	7	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 58
18	14:21:27.483000	9	-- --- ---	6	Building A	Motor	Control Unit	ACK	
19	14:21:29.483000	10	-- --- ---	7	Building B	Lamp	Control Unit	ACK	
20	14:21:31.483000	13	-- --- ---	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
21	14:21:33.483000	13	-- --- ---	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
22	14:21:35.483000	13	-- --- ---	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
23	14:21:37.483000	13	-- --- ---	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
24	14:21:39.483000	10	PR ---	-	Building A	Control Unit	*/*	UnACKD	UPDT[Motor Speed] 00
25	14:21:41.483000	12	PR ---	-	Building B	Control Unit	*/*	UnACKD	UPDT[Light Intensity] FF FF

Abbildung 23: Logfenster einer Paketlogdatei

Sie können nun die Logdatei weiter analysieren oder die LPA-Software mittels [Menü File | Exit] beenden.

4 Verwendung des LPAs

Der LOYTEC Protokollanalyser ermöglicht die Beobachtung und Analyse des Verkehrs eines CEA-709-Netzwerks durch Aufzeichnung und Speicherung der Pakete, welche am Netzwerk verschickt werden. Der LPA ist eine Applikation mit Multidokumentenschnittstelle (MDI, *Multi Document Interface*). Dies bedeutet, dass mehrere Dokumente (Paketlogs) gleichzeitig geöffnet werden können. Die Paketlogs sind in Logdateien gespeichert. Es existiert ein spezieller Paketlog, der als 'Aktiver Log' ('Active Log') bezeichnet wird. Im entsprechenden Logfenster werden die gerade aufgezeichneten Pakete angezeigt. Es kann immer nur ein aktiver Log existieren. Ein neuer aktiver Log wird mittels [Menü File | New] oder per Klick auf den Knopf  erzeugt. Abbildung 24 zeigt das LPA-Hauptfenster mit zwei geöffneten Logdateien.

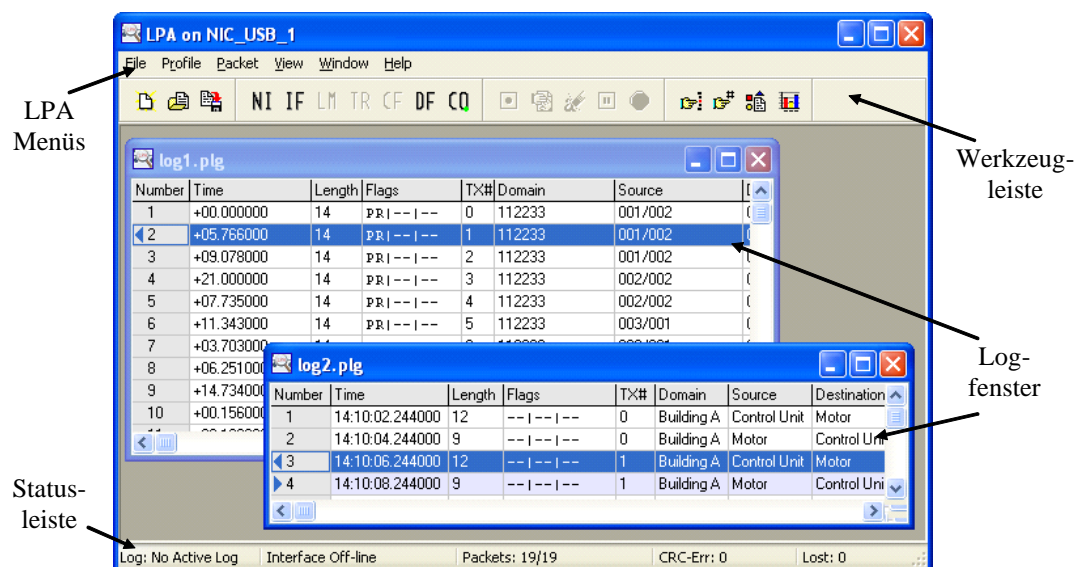


Abbildung 24: LPA-Hauptfenster

4.1 LPA Menüs

Hier können alle Funktionen des LPAs aufgerufen werden. Für die meisten Menüpunkte existieren zusätzlich Tastenkombinationen, welche neben den entsprechenden Menüpunkten angezeigt werden. Die fünf Hauptmenüs des LPAs enthalten folgende Funktionsgruppen:

File-Menü: Logdateiverarbeitung und allgemeine Einstellungen,

Profile-Menü: Interface- und Log-Einstellungen,

<i>Packet-Menü:</i>	Paketaufzeichnung und -analyse,
<i>View-Menü:</i>	Funktionen gleich Kontextmenü, siehe Abschnitt 4.6,
<i>Window-Menü:</i>	Arrangement der Logfenster und des sichtbaren Logfensters,
<i>Help-Menü:</i>	Inhalt der Hilfedatei und Informationen über die LPA-Software.

Je nach Zustand des LPAs können einige Menüpunkte deaktiviert sein, wenn die entsprechende Funktion gerade nicht verfügbar ist. Für die folgende Beschreibung aller Funktionen des LPAs wird auch immer der entsprechende Menüpunkt zum Aufruf der Funktion genannt.

4.2 Werkzeugleiste

Die wichtigsten Funktionen der LPA-Software können in der Werkzeugleiste per Mausclick aktiviert werden. Sobald sich der Mauszeiger über einem der Knöpfe befindet, erscheint der Name des entsprechenden Menüpunkts, siehe Abbildung 25.

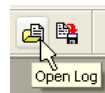


Abbildung 25: **Knopf mit zugehörigem Menüpunkt**

Einige Knöpfe können zeitweise deaktiviert sein, wenn die entsprechenden Menüpunkte gerade nicht verfügbar sind. Die Werkzeugleiste besteht aus folgenden Knöpfen:



New Log [Menü File | New]: Erzeugt ein neues Fenster für den aktiven Log. Dies ist nötig, um Pakete vom Netzwerk oder von anderen Quellen (siehe Kapitel 5) aufzuzeichnen.



Open Log [Menü File | Open...]: Öffnet eine zuvor gespeicherte Logdatei.



Save Log [Menü File | Save]: Speichert den aktuellen Log in eine Logdatei. Um den Log unter einem neuen Namen zu speichern, verwenden Sie [Menü File | Save As...].



Network Interface [Menü Profile | Interface...]: Auswahl des Netzwerk-Interfaces (siehe Kapitel 2).



Interface Settings [Menü Profile | Interface...]: Ruft die Interface-Einstellungen auf (siehe Kapitel 2).



Log Mode [Menü Profile | Log Mode...]: Erlaubt die Einstellung des Logmodus für den aktiven Log, bevor der Logprozess gestartet wird (siehe Abschnitt 5.1).



Trigger [Menü Profile | Trigger...]: Öffnet den Pakettrigger des aktiven Logs. Dieser entscheidet, wann der Logprozess gestartet werden soll (siehe Abschnitt 5.3). Ein kleiner grüner Punkt auf dem Knopf zeigt an, ob der Pakettrigger aktiviert ist.



Capture Filter [Menü Profile | Capture Filter...]: Öffnet das Aufzeichnungsfiler des aktiven Logs. Während des Logprozesses entscheidet dieses, ob eintreffende Pakete gespeichert oder verworfen werden (siehe Abschnitt 5.3). Ein kleiner grüner Punkt auf dem Knopf zeigt an, ob das Aufzeichnungsfiler aktiviert ist.



Display Filter [Menü Profile | Display Filter...]: Öffnet das Anzeigefilter des aktuellen Logs. Dieses entscheidet, ob gespeicherte Pakete letztlich im Logfenster angezeigt werden (siehe Abschnitt 5.3). Ein kleiner grüner Punkt auf dem Knopf zeigt an, ob das Anzeigefilter aktiviert ist.



Converter [Menü Profile | Converter...]: Öffnet den Paketkonverter des aktuellen Logs. Dieser wird verwendet, um die im Paket enthaltenen Nummern in symbolische Namen umzusetzen (siehe Abschnitt 5.2). Ein kleiner grüner Punkt auf dem Knopf zeigt an, ob ein Paketkonverter aktiviert ist.



Start Log from Network [Menü Packet | Start Log | Network]: Startet einen Paketlog vom angeschlossenen Netzwerk. Pakete werden solange aufgezeichnet, bis der Log unterbrochen oder beendet wird. Ein Log kann nur gestartet werden, wenn ein aktives Logfenster existiert.



Pause Update [Menü Packet | Pause Update]: Hält die Aktualisierung der Anzeige im Logfenster, im Paketstatistikfenster (siehe Abschnitt 5.5) sowie auf der Statusleiste während des Logprozesses an.



Clear Log [Menü Packet | Clear Log]: Löscht alle Pakete des aktiven Logs. Dies ist nur möglich, wenn der Logvorgang vorher unterbrochen wurde (siehe nächsten Knopf).



Pause Log [Menü Packet | Pause Log]: Unterbricht den Logvorgang, bis der Knopf erneut gedrückt wird. Solange der aktive Log unterbrochen ist, können die Konverter- und Filterparameter sowie die Anzeigeeoptionen editiert werden (siehe Kapitel 5).



Stop Log [Menü Packet | Stop Log]: Beendet den Logvorgang. Der aktive Log wird inaktiv und kann dann in eine Logdatei gespeichert werden. Um den Logvorgang erneut zu starten, muss zuvor ein neues Logfenster erzeugt werden.



Find [Menü Packet | Find...]: Erlaubt die Suche nach einem bestimmten Paket im aktuellen Logfenster. Um die Suche fortzusetzen, nachdem ein passendes Paket gefunden wurde, drücken Sie F3 oder wählen [Menü Packet | Find Next].



Go To [Menü Packet | Go To...]: Erlaubt ein bestimmtes Paket durch Eingabe der entsprechenden Zeilennummer anzuspringen.



Display Options [Menü View | Display Options...]: Erlaubt das Einstellen der Anzeigeeoptionen, welche die Darstellung bestimmter Informationen des aktuellen Logfensters beeinflussen (siehe Abschnitt 5.4).



Statistics [Menü Packet | Statistics]: Zeigt das Paketstatistikfenster des aktuellen Logs an. Dieses beinhaltet auch die Knotenstatistik, Reports und Trends.

Der Pakettrigger sowie die Aufzeichnungs- und Anzeigefilter können per rechtem Mausclick auf den entsprechenden Knopf aktiviert und deaktiviert werden, sowie auch innerhalb des zugehörigen Filterdialogfensters (per linker Maustaste aufrufbar).

4.3 Logfenster

Ein Logfenster zeigt Paketdaten in verschiedenen Formen. Es besteht aus bis zu drei Bereichen, siehe Abbildung 26.

Pakettabelle

The screenshot shows the 'Active Log Running' window with three main sections:

- Pakettabelle (Packet Table):** A table with columns: Number, Time, Length, Flags, TX#, Domain, Source, Destination, Service, Data. Row 3 is selected.
- Paketdetails (Packet Details):** A panel on the left showing general information for Packet Number 3, including time, length, TX number, and service.
- Protokolldetails (Protocol Details):** A tree view on the right showing the protocol stack for the selected packet, including PDU, NPDU, and APDU headers.

Arrows point from the labels 'Pakettabelle', 'Paketdetails', and 'Protokolldetails' to their respective sections in the screenshot.

Abbildung 26: Logfenster

Pakettabelle

Dabei handelt es sich um die Paketliste im oberen Bereich des Logfensters. Sie ist immer sichtbar und zeigt die wichtigsten Informationen jedes Pakets an, wobei jede Zeile der Tabelle ein Paket repräsentiert. Die angezeigten Informationen beinhalten:

- *Number*: die Zeilennummer des Pakets,
- *Time*: den Zeitstempel (Zeitpunkt des Paketempfangs),
- *Length*: die Paketlänge in Bytes,
- *Flags*: die Paketflags (Priority | Alternate Path | Authenticated | Idempotent),
- *TX#*: die Transaktionsnummer, falls im Paket enthalten,

- *Domain*: die Domain, in welcher das Paket versendet wurde,
- *Source*: die Absenderadresse des Pakets,
- *Destination*: die Empfängeradresse des Pakets,
- *Service*: das Service, welches zum Pakettransport verwendet wurde,
- *Data*: die Daten, welche im Paket transportiert werden.

In der 'Number'-Spalte werden Pakete einer bestimmten Transaktion mittels kleiner Dreiecke identifiziert. Ein Dreieck, welches nach links zeigt, kennzeichnet das erste Paket der Transaktion. Bei allen folgenden Paketen zeigt das Dreieck nach rechts. Zusätzlich werden alle zusammengehörigen Pakete blau markiert.

Die Auflösung der Zeitstempel (Time) beträgt 1 μ s bei NIC709 Netzwerk-Interfaces. Andere Netzwerk-Interface-Typen können niedrigere Zeitstempelauflösung haben, siehe Abschnitt 2.3. Beachten Sie, dass Pakete ihren Zeitstempel kurz vor Empfang des ersten Bits erhalten (bei Empfang des Startbits). Bei den Adressen (Source, Destination) trennt ein Querstrich das Subnet von der Knotennummer oder NID (z.B.: <Subnet>/<Knotennummer>), Gruppen wird eine Raute vorangestellt (#<group>) und Broadcasts werden mittels Sternzeichen angezeigt (z.B.: <Subnet>/* oder */*). Jedes fehlerhafte Paket (mit Protokollfehler, z.B. CRC-Fehler) wird stets rot in der Pakettabelle angezeigt. Der entsprechende Fehler wird dabei in der Datenspalte (Data) angezeigt. SNVT-Nachrichten (Standardnetzwerkvariablentypen), werden in übersetzter Form (statt der entsprechenden Zahlen) in der Datenspalte angezeigt. Dazu muss allerdings zuvor der SNVT der Netzwerkvariable im Knoteneditor des Paketkonverters (siehe Abschnitt 5.2) ausgewählt worden sein.

Paketdetails

Diese Sektion im unteren Bereich des Logfensters zeigt detaillierte Informationen über das gerade ausgewählte Paket an. Neben generellen Paketinformationen werden Adress- und Nachrichteninformationen sowie die transportierten Daten dargestellt. Letztere werden in dem Fenster ganz unten in Listenform sowohl numerischer als auch textuell (ASCII) angezeigt. Netzwerkmanagement und -diagnosenachrichten werden dabei gemäß des Protokolls übersetzt. Da sich die Code-Bereiche für Applikations-, Netzwerkmanagement- und -diagnosenachrichten überschneiden, müssen Sie die Interpretationsart manuell wählen. Ist dies der Fall, so erscheinen am unteren Ende der Paketdetails drei kleine Knöpfe, welche eben diese Auswahl ermöglichen (*Application*, *Management* oder *Diagnostic*), siehe Abbildung 27.

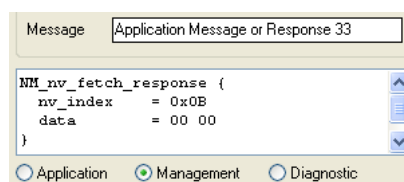


Abbildung 27: **Netzwerkmanagement- und -diagnosenachrichten**

Aktualisierungsnachrichten von SNVTs (Standardnetzwerkvariablentypen) werden ebenfalls übersetzt und korrekt angezeigt (siehe Abbildung 28). Wie bereits erwähnt, ist dies jedoch nur möglich, wenn sowohl ein symbolischer Name sowie ein SNVT für die entsprechende Netzwerkvariable im Paketkonverter (siehe Abschnitt 5.2) eingestellt sind. Wenn eine SNVT-Nachricht angezeigt wird, können Sie die Interpretationsform am unteren Ende der Paketdetails wählen: 'Raw' bedeutet, dass keine Übersetzung stattfindet. 'Structure' bedeutet, dass zwar die korrekte SNVT-Struktur angezeigt wird, die enthaltenen Werte jedoch nicht übersetzt werden. 'Converted' bedeutet schließlich, dass auch die enthaltenen Werte gemäß der SNVT-Master-List übersetzt werden. Beachten Sie, dass als

Meßsystem in den LPA-Einstellungen sowohl SI-System als auch Imperiales US-System gewählt werden kann, siehe Abschnitt 5.11.

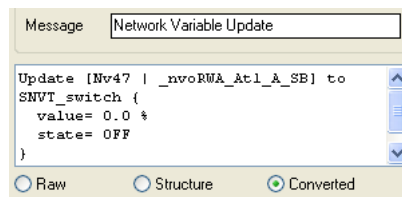


Abbildung 28: SNVT-Nachrichten

Protokolldetails

Diese Sektion ist ebenfalls unterhalb der Pakettabelle angeordnet und zeigt protokollschichtspezifische Informationen über das gerade ausgewählte Paket an. Jede Schicht (PPDU, NPDU, TPDU, SPDU, AuthPDU und APDU) kann dabei aufgeklappt werden, um alle Informationen bis auf die Ebene einzelner Bits preiszugeben. Unterhalb der Protokolldetails wird zusätzlich das gesamte Paket in hexadezimaler Form angezeigt. Der hervorgehobene Bereich entspricht dabei immer dem gerade ausgewählten Protokolldetail.

Sowohl die Paket- als auch die Protokolldetails können jederzeit über das Kontextmenü ein- und ausgeblendet werden (erreichbar über rechte Maustaste).

4.4 Statusleiste

Dies ist die Leiste am unteren Ende des LPA-Hauptfensters. Hier werden Informationen über den gerade aktiven Log bzw. den letzten aktiven Log (falls noch kein neuer gestartet wurde) angezeigt. Abbildung 29 zeigt die Statusleiste des LPAs.

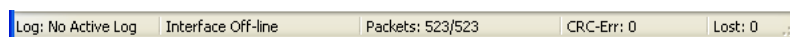


Abbildung 29: Statusleiste

Log:

Hier wird der Status des aktiven Logs angezeigt. Mögliche Werte sind: 'No Active Log' (es existiert kein aktiver Log), 'Not Running' (es existiert ein aktives Logfenster, es werden jedoch im Moment keine Pakete aufgezeichnet), 'Running On-line' (empfangene Pakete werden aufgezeichnet und im Logfenster angezeigt) und 'Running Off-line' (Pakete werden aufgezeichnet, das Log- und das Statistikenfenster werden jedoch im Moment nicht aktualisiert). Der Logstatus ändert sich wann immer Sie [Menü Packet | Start Log], [Menü Packet | Pause Update] oder [Menü Packet | Pause Log] wählen. Er wird außerdem von den Logmuseinstellungen (siehe Abschnitt 5.1) beeinflusst.

Transceiver:

Dies ist das Feld rechts neben dem 'Log:'-Feld. Hier wird der Transceiver angezeigt, welchen Sie in den Interface-Einstellungen ausgewählt haben, sobald eine Paketaufzeichnung erfolgt. Solange keine Pakete aufgezeichnet werden, wird die Meldung „Interface Off-line“ angezeigt.

Packets:

Hier sehen Sie die Anzahl der gespeicherten Pakete, die das Aufzeichnungsfilter (siehe Abschnitt 5.3) passiert haben, sowie die Zahl aller empfangenen Pakete im Format <gespeichert>/<alle>. Im Unterschied zu den Werten der Paketstatistik (siehe Abschnitt 5.5) werden diese Werte nicht gelöscht, wenn Sie im Statistikenfenster auf 'Clear' klicken.

Auf diese Weise können Sie immer den absoluten Wert der empfangenen Pakete einsehen, selbst wenn die Statistikdaten gelöscht wurden. Dasselbe gilt auch für die im nächsten Abschnitt beschriebenen CRC-Fehler.


CRC-Err:

Hier wird die Anzahl aller empfangenen Pakete mit CRC-Fehler angezeigt.

Lost:

Hier wird die Anzahl der verlorenen Pakete angezeigt (siehe Abschnitt 5.5).

4.5 Suchen und Anspringen von Paketen

Sie können nach einem bestimmten Paket im aktuellen Logfenster durch Auswahl von [Menü Packet | Find...] oder Klick auf den Knopf  suchen.

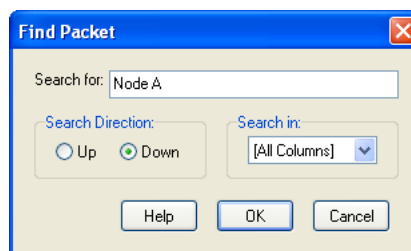


Abbildung 30: Suchen von Paketen

Das entsprechende Dialogfenster ist in Abbildung 30 zu sehen. Es besteht aus folgenden Feldern:

Search for:

Hier können Sie den Suchbegriff eingeben, nach welchem in der Pakettabelle des aktuellen Logfensters gesucht werden soll. Groß-/Kleinschreibung wird bei der Suche nicht beachtet.


Search Direction:

Die Suche beginnt immer beim gerade ausgewählten Paket der Pakettabelle. Hier können Sie die Suchrichtung angeben ('Up'=aufwärts, 'Down'=abwärts).

Search in:

Hier können Sie die Spalte auswählen, in der gesucht werden soll. Sie können die Suche auch über alle Spalten erstrecken ('[All Columns]').

Sobald Sie auf 'OK' klicken, wird das erste gefundene Paket markiert. Sie können dann mit der Taste F3 oder mit [Menü Packet | Find Next] nach dem nächsten Paket suchen.

Es ist ebenfalls möglich, durch Auswahl von [Menü Packet | Go To...] oder Klick auf den Knopf , direkt zu einem Paket einer bestimmten Zeilennummer ('Packet Number') zu springen. Abbildung 31 zeigt das entsprechende Dialogfenster.

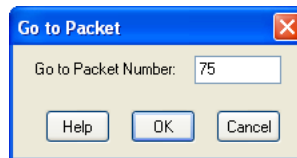


Abbildung 31: Anspringen von Paketen

4.6 Funktionen des Kontextmenüs (View-Menüs)

Das Kontextmenü erscheint, wenn Sie mit der rechten Maustaste in ein Logfenster klicken oder das [Menü View] aufrufen, siehe Abbildung 32.

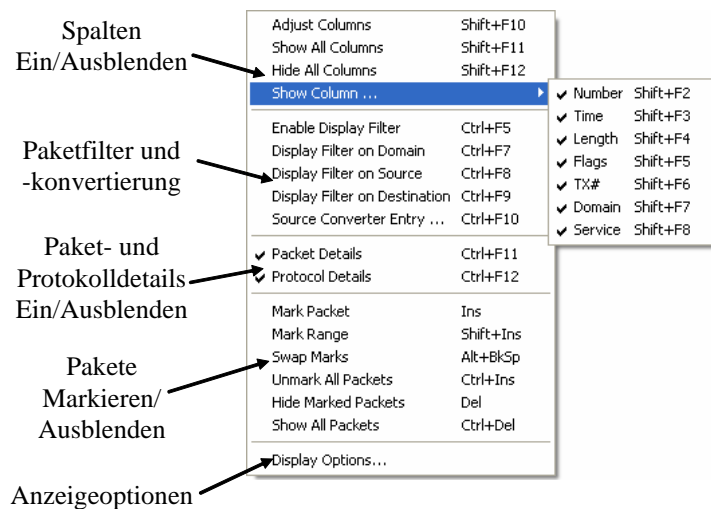


Abbildung 32: Kontextmenü (View-Menü)

Das Kontextmenü bietet grundsätzlich fünf Funktionen:

Spalten Ein/Ausblenden

Hier können Sie auswählen ('Show Column ...'), welche Spalten der Pakettabelle und somit welche Paketinformationen angezeigt werden sollen. Wenn Sie 'Show all Columns' auswählen, werden alle Spalten eingeblendet. Wenn Sie 'Hide all Columns' auswählen, werden alle Spalten außer der Absenderadresse (Source), der Empfängeradresse (Destination) und den Daten ausgeblendet. Durch Klick auf 'Adjust Columns' kann die Spaltenbreite aller Spalten den aktuell angezeigten Daten angepasst werden.

Paketfilter und -konvertierung

Wenn Sie 'Display Filter on Domain' auswählen, wird automatisch ein Anzeigefilter generiert, welches nur Pakete der Domain anzeigt, welche im aktuell ausgewählten Paket enthalten ist. Mit 'Display Filter on Source' werden nur jene Pakete angezeigt, welche vom ausgewählten Absenderknoten ('Source') gesendet oder empfangen wurden, mit 'Display Filter on Destination' nur jene Pakete, die zum oder vom Empfänger (Knoten, Subnet oder Gruppe) übertragen wurden. Um das Anzeigefilter zu deaktivieren und wieder alle Paket anzuzeigen, entfernen Sie den Haken bei 'Enable Display Filter'. Das zuletzt generierte Filter kann durch Aktivieren von 'Enable Display Filter' wiederhergestellt werden. Durch Klick auf 'Source Converter Entry...' wird der Paketkonverter für den aktuell ausgewählten Absenderknoten angezeigt. Damit kann auf einfache Weise der Konvertereintrag eines Knoten geändert bzw. neu erstellt werden. Weiterführende Informationen über Paketfilter und -konverter sind in den Abschnitten 5.2 und 5.3 zu finden.

Paket- und Protokolldetails Ein/Ausblenden

Beachten Sie, dass wenn sowohl die Paketdetails ('Packet Details') als auch die Protokolldetails ('Protocol Details') eingeblendet sind, beide Bereiche nebeneinander unterhalb des Logfensters angezeigt werden (siehe Abbildung 26).

Pakete Markieren/Ausblenden



Hier können Sie einzelne Pakete ('Mark Packet') sowie Paketbereiche ('Mark Range') in der Pakettabelle markieren und demarkieren. Dies ist alternativ auch per Doppelklick auf ein bestimmtes Paket bzw. durch Drücken der SHIFT-Taste während eines Doppelklicks (für Paketbereiche) möglich. Markierte Pakete können mittels 'Hide Marked Packets' ausgeblendet werden. Alle Markierungen können mittels 'Unmark All Packets' wieder verworfen werden, ausgeblendete Pakete können mittels 'Show All Packets' wieder eingeblendet werden. Sie können jederzeit die Anzahl der markierten und ausgeblendeten Pakete im Statistikfenster (siehe Abschnitt 5.5) des aktuellen Logs einsehen. Beachten Sie, dass markierte Pakete stets grün angezeigt werden.

Anzeigeoptionen


Hier können Sie die Anzeigeoptionen aufrufen, siehe Abschnitt 5.4.

Alle Funktionen des Kontextmenüs können auch über die im Menü angezeigten Tastenkombinationen aufgerufen werden.

4.7 Paketaufzeichnung vom Netzwerk

Um Pakete von einem Netzwerk aufzuzeichnen, müssen Sie zunächst ein neues aktives Logfenster erzeugen (-Knopf). Nachdem Sie den Logprozess mittels [Menü Packet | Start Log | Network] oder durch Klick auf  gestartet haben, werden empfangene Pakete im Paketpuffer gespeichert. Wenn Sie den 'On-line'-Modus aktiviert haben (was standardmäßig der Fall ist, siehe Abschnitt 5.1), können Sie eintreffende Pakete im Logfenster beobachten. Sollte der 'On-line'-Modus deaktiviert sein, so können Sie gespeicherte Pakete nur betrachten, solange der Log unterbrochen ist; während des Logprozesses bleibt das Logfenster leer. Die Anzahl der empfangenen sowie gespeicherten Pakete kann jederzeit im Statistikfenster (siehe Abschnitt 5.5) oder auf der Statusleiste eingesehen werden.


4.8 Logdateien

Eine Logdatei wird immer dann erzeugt, wenn Sie [Menü File | Save] oder [Menü File | Save As...] aufrufen sowie auf den -Knopf klicken. Standardmäßig hat jede Logdatei die Endung '.plg'. Die Datei enthält grundsätzlich alle Pakete des Logs, nicht nur jene, die das Anzeigefilter passiert haben (und daher gerade im Logfenster sichtbar sind, siehe Abschnitt 5.3).

Zusätzlich zu den Paketdaten werden noch folgende Informationen in der Logdatei gespeichert:

- der Pfad der Paketkonverterdatei falls vorhanden (siehe Abschnitt 5.3),
- der Pfad der Anzeigefilterdatei falls vorhanden (siehe Abschnitt 5.3),
- die gerade ausgewählte Zeilennummer in der Pakettabelle des Logfensters,

- die Anzeigeoptionen (siehe Abschnitt 5.4),
- Breite und Sichtbarkeit der Spalten der Pakettabelle,
- Sichtbarkeit der Paket- und Protokolldetails im Logfenster,
- markierte und ausgeblendete Pakete,
- der Statistiktrend (nur in Logdateien von LPA 3.0 oder höher, siehe Abschnitt 5.8),
- einige zusätzliche Statistikwerte (nur in Logdateien von LPA 3.0 oder höher),
- Anzeigeoptionen des Statistikfensters (nur in Logdateien von LPA 3.0 oder höher).

Wann immer Sie eine bereits existierende Logdatei speichern, werden diese Werte überschrieben. Wenn Sie eine Logdatei mittels [Menü File | Open...] oder Klick auf  öffnen, werden auch automatisch die entsprechenden Konverter- und Filterdateien geöffnet, falls sie im gespeicherten Pfad noch existieren. Logdateien können (genau wie Packet-Recording-Dateien, siehe Abschnitt 5.10) auch als Quelle für neue Paketlogs dienen.

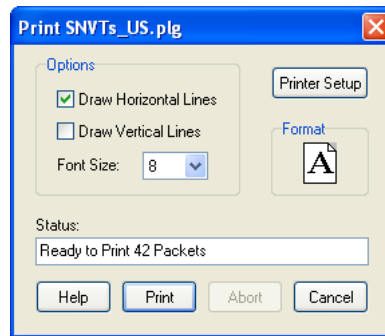
Trotz der neuen Informationen, welche in Logdateien des LPA 3.0 (oder höher) gespeichert werden, bleiben die Logdateien sowohl abwärts- als auch aufwärtskompatibel. Dies bedeutet, dass jede Logdatei mit jedem LPA angezeigt werden kann, unabhängig von den Versionen der Datei und der LPA-Software.

4.9 Exportieren einer Logdatei

Durch Auswahl von [Menü File | Export...] können Sie die Pakettabelle des aktuellen Logfensters als CSV-Datei (Comma Separated Value) exportieren. Falls Sie nur bestimmte Pakete bzw. Spalten exportieren wollen, benutzen Sie bitte das Anzeigefilter (siehe Abschnitt 5.3) sowie die Funktionen des Kontextmenüs. In der ersten Zeile der exportierten Datei werden immer die Namen der exportierten Spalten gespeichert. Zeilen (Pakete) werden mittels Zeilenumbruch getrennt. Die Trennzeichen für Spalten und Dezimalstellen können in den LPA-Einstellungen gewählt werden (siehe Abschnitt 5.11). Die so exportierten Dateien können dann z.B. in Tabellenkalkulationsprogrammen weiterverwendet werden.

4.10 Drucken einer Logdatei

Durch Auswahl von [Menü File | Print...] können Sie die Pakettabelle des aktuellen Logfensters ausdrucken. Oft ist vor dem Drucken eine Reduktion der darzustellenden Pakete mittels Anzeigefilter (siehe Abschnitt 5.3) und der Ausblendfunktion des Kontextmenüs sinnvoll. Um die Paketinformation auf die zur Verfügung stehende Papierbreite zu reduzieren, benutzen Sie bitte die Anzeigeoptionen sowie die Spaltenausblendfunktion des Kontextmenüs. Das Druckfenster ist in Abbildung 33 dargestellt.

Abbildung 33: **Print Log**

Innerhalb des Druckfensters können Sie die Größe der Schriftart wählen sowie auf Querformat umstellen (durch Klick auf 'Printer Setup'). Zusätzlich haben Sie die Option, horizontale ('Draw Horizontal Lines') und vertikale ('Draw Vertical Lines') Trennungslinien zu drucken. Sind die Zeilen der Pakettabelle zu breit, um auf das Papier zu passen, so kann nicht gedruckt werden und die Meldung 'Packets will not fit on Paper' wird angezeigt. Während des Druckvorgangs kann der Fortschritt beobachtet sowie jederzeit der Vorgang abgebrochen werden.

4.11 Hilfedatei

Um die Hilfedatei des LPAs aufzurufen, wählen Sie [Menü Help | Help Topics]. Wenn Sie innerhalb eines bestimmten Dialogfensters auf den 'Help'-Knopf klicken, erhalten Sie spezifische Hilfe für dieses Fenster. Um generelle Informationen über die LPA-Software zu erhalten, können Sie außerdem [Menü Help | About LPA...] sowie [Menü Help | Contact...] wählen.

5 Erweiterte Funktionen des LPAs

Zusätzlich zur Aufzeichnung und Darstellung von Paketinformationen bietet der LPA auch erweiterte Funktionen, wie Paketfiltrierung, -konversion, -statistik und -simulation. Die folgenden Abschnitte beschreiben die Bedeutung dieser Begriffe sowie die Verwendung der entsprechenden Funktionen.

5.1 Logmodus

Bevor Sie einen Paketlog starten, können Sie einige Einstellungen - den Paketaufzeichnungsmodus sowie die Anzeigeaktualisierung betreffend - vornehmen. Wählen Sie dazu [Menü Profile | Log Mode...] oder klicken Sie auf den Knopf **LM**. Das entsprechende Dialogfenster ist in Abbildung 34 zu sehen.

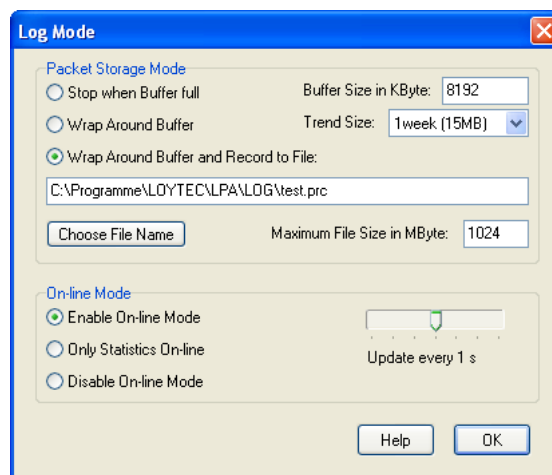


Abbildung 34: Logmodus

Packet Storage Mode

Hier können Sie angeben, wie empfangene Pakete gespeichert werden sollen sowie wie viel Speicher als Paketpuffer zur Verfügung gestellt werden soll. Zusätzlich können Sie die Puffergröße für den Statistiktrend (siehe Abschnitt 5.8) im Feld 'Trend Size' einstellen. Drei Modi zur Paketspeicherung sind verfügbar: 'Stop when Buffer full' bedeutet, dass der Log automatisch beendet wird, sobald der Paketpuffer voll ist. Im 'Wrap around Buffer'-Modus werden im Stil eines Ringpuffers jeweils die ältesten Pakete im Speicher von neuen überschrieben. Die Größe des zu verwendenden Paketpuffers im Hauptspeichers kann oben rechts in KBytes (bis maximal 128 MB) angegeben werden. Im dritten Modus 'Wrap around Buffer and Record to File' können zusätzlich alle empfangenen Pakete in eine Packet-Recording-Datei gespeichert werden. Eine Packet-Recording-Datei (*.prc) speichert alle eintreffenden Pakete bereits während des Logprozesses, siehe Abschnitt 5.10. Die

maximale Größe der Packet-Recording-Datei kann in Mbytes (bis zu 16 GB) im Feld 'Maximum File Size in Mbyte' konfiguriert werden.

On-line Mode

'Enable On-line Mode' bedeutet, dass empfangene Pakete während des Logvorgangs beobachtet werden können. Falls Ihr PC mit der Paketgeschwindigkeit nicht Schritt hält, können Sie versuchen, die Aktualisierung der Anzeige komplett auszuschalten ('Disable On-line Mode') bzw. nur die Aktualisierung für die Paketstatistik einzuschalten ('Only Statistics On-line'). Im 'On-line'-Modus können Sie außerdem das Aktualisierungsintervall für das Logfenster sowie die Statistik auswählen ('Update every ...').

5.2 Paketkonverter

Jedem Logfenster ist automatisch ein Paketkonverter zugeordnet, womit symbolische Namen für Netzwerkadressen und -variablen vergeben werden, um den Paketinhalt leichter verständlich darstellen zu können. Dazu werden im Logfenster diese symbolischen Namen statt der im Paket enthaltenen Zahlen angezeigt. Die entsprechenden Konvertertabellen können als Konverterdateien gespeichert werden, welche die Endung '.pco' besitzen. Beachten Sie, dass mehreren Logdateien dieselbe Konverterdatei zugeordnet werden kann. Wenn Sie den Konverter innerhalb eines Logs editieren und speichern, so verändert dies automatisch auch die Konverterfunktionalität für alle anderen Logdateien, denen diese Konverterdatei zugeordnet ist. Falls Sie dies nicht wünschen, so müssen Sie den editierten Konverter unter einem neuen Namen speichern. Konverterdateien können zusammengefügt werden, indem zunächst eine Datei geöffnet, alle weiteren dann mittels „Merge“ hinzugefügt werden. Beachten Sie außerdem, dass Sie einen Standardkonverter in den LPA-Einstellungen (siehe Abschnitt 5.11) setzen können, welcher dann immer automatisch nach dem Start der Software verwendet wird.



Der Paketkonverter des aktuellen Logfensters kann mittels [Menü Profile | Converter...] oder per Klick auf den Knopf  editiert werden. Ein kleiner grüner Punkt in der rechten unteren Ecke des Knopfs  zeigt an, dass Konvertertabellen eingegeben wurden (der Konverter also nicht leer ist) und der Konverter aktiviert ist. Sie können den Konverter aktivieren und deaktivieren, indem Sie auf 'Enable Converter' klicken. Außerdem kann der Konverter für eine bestimmte Domain, ein Subnet, einen Knoten oder eine Gruppe direkt im Knotenstatistikfenster (siehe Abschnitt 5.6) oder mittels Kontextmenü der Pakettabelle (Abschnitt 4.6) aufgerufen werden. Bitte beachten Sie, dass Änderungen am Paketkonverter nicht rückgängig gemacht werden können (per 'Cancel'), wenn die Option 'Backup Converter Settings' in den LPA-Einstellungen ausgeschaltet ist, siehe Abschnitt 5.11.

Abbildung 35 zeigt das Dialogfenster zur Eingabe der Paketkonverterdaten. In allen vier Tabellen des Konverters können Sie Zeilen löschen, indem Sie die *erste* Spalte der entsprechenden Zeile auswählen und ENTF drücken. Auf dieselbe Weise können Sie Zeilen einfügen, per Druck auf EINFÜG. Alle Tabellen außer der Knotentabelle (ganz unten) können direkt durch Drücken der RETURN-Taste oder per Klick ins entsprechende Feld editiert werden. Sie können alle Tabellen jederzeit per Klick auf den Knopf 'Clear' löschen.

Jede Zeile der Konvertertabellen beginnt mit einem symbolischen Namen der entsprechenden Domain, des Subnets, der Gruppe oder des Knotens. Diese symbolischen Namen müssen mit einem nicht-numerischen Zeichen beginnen und dürfen ansonsten jedes Zeichen außer ':', '=', '\$', '#', '/' und '*' enthalten. Es existieren vier Konvertertabellen: *Domains*, *Subnets*, *Groups* und *Nodes*.

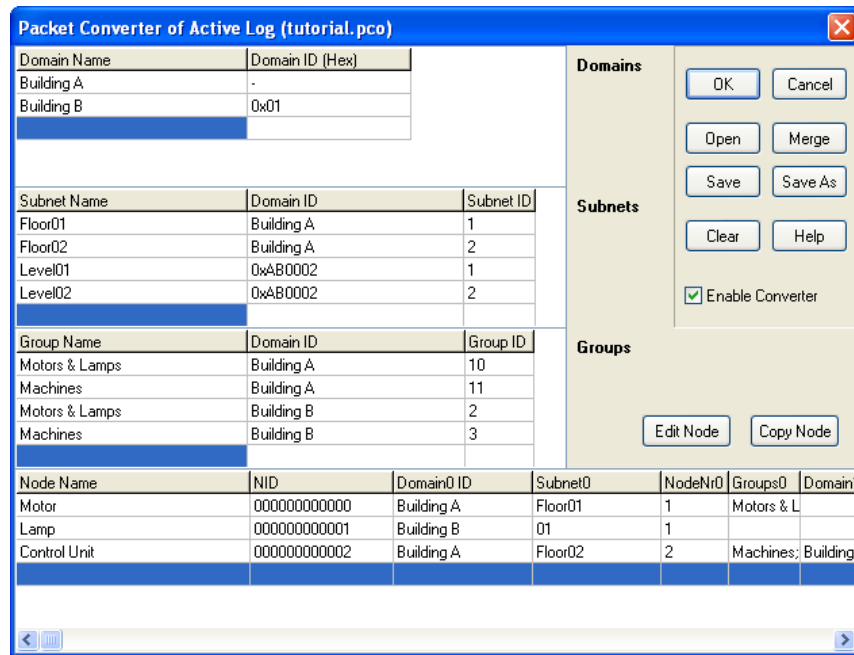


Abbildung 35: Paketkonverter

Domains

Hier können Sie den Domain-IDs symbolische Domainnamen zuordnen. Die Domain-ID muss immer hexadezimal in einem der folgenden Formate, gemäß dem Netzwerkprotokoll, eingegeben werden: 0xHH, 0xHHHHHHH oder 0xHHHHHHHHHHHHHH, wobei 'H' für eine hexadezimale Ziffer steht. Zusätzlich können Sie '--' eingeben, um die Domain-ID mit Länge 0 zu spezifizieren.

Subnets

In jeder Zeile der Subnet-Tabelle können Sie einer Subnet-ID einen symbolischen Subnet-Namen zuordnen. Sie müssen außerdem immer die entsprechende Domain-ID für jedes Subnet angeben. Subnet-IDs können dezimal (z.B.: 123) oder hexadezimal (z.B.: 0xAB) eingegeben werden. Die Domain-ID kann hier als symbolischer Name (aus der Domaintabelle) oder hexadezimal, wie oben beschrieben, eingegeben werden.

Groups

Wie bei den Subnets können Sie hier den Gruppen-IDs symbolische Gruppennamen zuordnen. Gruppen-IDs können genau wie Subnet-IDs dezimal (z.B.: 123) oder hexadezimal (z.B.: 0xAB) eingegeben werden.

Nodes

Dies ist die Knotentabelle im unteren Bereich des Konverterfensters. Um einen Knoten (Node) zu editieren, müssen Sie auf 'Edit Node' klicken oder in die entsprechende Zeile der Knotentabelle doppelklicken. Sie können auch einen bereits bestehenden Knoten per Klick auf 'Copy Node' kopieren. In beiden Fällen wird anschließend der Knoteneditor aufgerufen, siehe Abbildung 36.

The screenshot shows the 'Node Editor' window for a node named 'Control Unit'. The NID is '000000000002'. There are two domain tables, Domain Table 0 and Domain Table 1. Domain Table 0 has Domain ID 'Building A', Subnet 'Floor02', and NodeNr '2'. Domain Table 1 has Domain ID 'Building B', Subnet '5', and NodeNr '8'. Both tables have a 'Groups' list with 'Machines' and 'Motors & Lamps' respectively. Below the tables is a 'Network Variables' table with columns: NV Name, Direction, Selector, SNVT, and Destination.

NV Name	Direction	Selector	SNVT	Destination
Motor Speed	Out	1	SNVT_motor_state	
Light Intensity	Out	2	SNVT_lux	
Switch1	In	61	SNVT_switch	

Abbildung 36: Knoteneditor

Node Name, NID und Node Info

Hier können Sie den Knotennamen und seine NID (Unique Node ID) eingeben. NIDs müssen stets hexadezimal im folgenden Format, gemäß dem Netzwerkprotokoll, eingegeben werden: 0xHHHHHHHHHHHH, wobei 'H' für eine hexadezimale Ziffer steht. Die ersten beiden Zeichen ('0x') sind hier optional. Sie können außerdem den Ort (Location) und eine Beschreibung (Description) des Knotens durch Klick auf den Knopf 'Node Info' angeben. Diese Information wird allerdings bei der Paketübersetzung nicht benutzt und hat auch keine Bedeutung im Netzwerkprotokoll. Sie soll nur als Hilfe dienen, um die Bedeutung jedes Knotens festzuhalten. Der Wert des 'Location'-Felds erscheint zusätzlich in der Titelleiste des Knoteneditorfensters.

Domain Tables

Jeder Knoten kann sich in bis zu zwei Domains befinden, welche in den Domaintabellen 0 und 1 konfiguriert werden. Sollte ein Knoten unkonfiguriert sein, können Sie diese Einträge einfach leer lassen. Für jede Domaintabelle können Sie die Domain-ID, das Subnet und die Knotennummer (NodeNr) eingeben. Zusätzlich können Sie jedem Knoten Gruppen zuordnen, indem Sie diese im Feld neben dem 'Add'-Knopf eingeben und schließlich auf 'Add' klicken. Die Gruppe erscheint dann in der darüber liegenden Liste. Um eine Gruppe wieder zu löschen, klicken Sie diese einfach an und drücken Sie ENTF. Domains, Subnets und Gruppen können als symbolische Namen (aus der entsprechenden Konvertertabelle) sowie in dezimaler oder hexadezimaler Form eingegeben werden.

Network Variables

Jede Zeile dieser Tabelle repräsentiert eine Netzwerkvariable des Knotens. Sie besteht aus dem Namen der Netzwerkvariable, ihrer Richtung und ihrem Selektor. Optional können Sie auch einen SNVT und eine Zieladresse angeben. Die Richtung einer Netzwerkvariable gibt an, ob es sich um eine Eingangs- oder Ausgangsnetzwerkvariable handelt. Mögliche Werte sind 'i', 'I' oder 'In' für Eingangsnetzwerkvariablen und 'o', 'O' oder 'Out' für Ausgangsnetzwerkvariablen. Der Selektor identifiziert eine Netzwerkvariable innerhalb eines Netzwerks. Er kann dezimal (z.B.: 12345) oder hexadezimal (z.B.: 0x0ABC) eingegeben werden. Tabelleneinträge können direkt durch Drücken der RETURN-Taste sowie durch Klicken ins entsprechende Feld editiert werden. Sie können eine Netzwerkvariable löschen, indem Sie die 'NV Name'-Spalte der entsprechenden Zeile

selektieren und ENTF drücken. Durch Druck auf EINFG können Sie auf dieselbe Weise eine Zeile einfügen.

Der SNVT (Standardnetzwerkvariablentyp) wird zur Interpretation von Update-Nachrichten der entsprechenden Netzwerkvariable verwendet. Die übersetzten Werte dieser Nachrichten werden dann sowohl in der Pakettabelle als auch in den Paketdetails des Logfensters angezeigt. Der SNVT kann direkt (als Name oder Nummer) eingegeben werden. Alternativ dazu kann er auch per Klick auf 'Select SNVT' (oder Doppelklick ins entsprechende Feld) aus einer Liste verfügbarer SNVTs ausgewählt werden. Wenn Sie keinen SNVT angeben wollen, lassen Sie das 'SNVT'-Feld der Netzwerkvariable einfach leer.

Das 'Destination'-Feld wird zur Unterscheidung von Netzwerkvariablen benutzt, die denselben Selektor besitzen. Die Zieladresse (Destination-Address) kann in einem der folgenden Formate eingegeben werden:

- Domainindex:0/* ... Netzwerkvariable mit domain-weitem Broadcast-Verhalten,
- Domainindex:Subnet/* ... Netzwerkvariable mit subnet-weitem Broadcast-Verhalten,
- Domainindex:Subnet/Knotennummer>... Netzwerkvariable geht an bestimmten Knoten,
- Domainindex:#Gruppe ... Netzwerkvariable wird an bestimmte Gruppe geschickt.

Der Domainindex spezifiziert einen der beiden Domaineinträge des aktuellen Knotens. Mögliche Werte sind 0 oder 1. Der Eintrag '0:#lamps' würde z.B. bedeuten, dass die Netzwerkvariable an die Gruppe 'lamps' im Domaintabelleneintrag 0 des gerade editierten Knoten geht. Beachten Sie, dass Sie neben dezimalen und hexadezimalen Werten auch symbolische Namen aus dem Paketkonverter für Subnets und Gruppen verwenden können. Wollen Sie keine Zieladresse für eine Netzwerkvariable angeben, so lassen Sie das 'Destination'-Feld einfach leer.

5.3 Paketfilter und -trigger

Ein Paketfilter entscheidet, ob ein Paket akzeptiert oder verworfen werden soll. Es wird verwendet, um die Menge an zu verarbeitenden Paketen zu reduzieren. Es gibt zwei Arten von Paketfiltern, das Aufzeichnungsfiler (Capture-Filter) und das Anzeigefilter (Display-Filter). Das Aufzeichnungsfiler entscheidet während eines aktiven Logs, ob ein empfangenes Paket gespeichert oder verworfen wird. Das Anzeigefilter entscheidet, welche der gespeicherten Pakete letztlich angezeigt werden. Beachten Sie, dass ein Anzeigefilter für bestimmte Domains, Subnets, Knoten und Gruppen auch automatisch mittels Knotenstatistik (siehe Abschnitt 5.6) oder Kontextmenü der Pakettabelle (Abschnitt 4.6) erstellt werden kann.

Das Aufzeichnungsfiler arbeitet nur, wenn ein aktiver Log läuft, wohingegen jedem Logfenster ein Anzeigefilter zugeordnet ist. Filterparameter können als Filterdateien gespeichert werden, welche die Endung '.pft' besitzen. Beachten Sie, dass mehreren Logdateien dieselbe Anzeigefilterdatei zugeordnet werden kann. Wenn Sie das Anzeigefilter innerhalb eines Logs editieren und speichern, so verändert dies automatisch auch die Filterfunktionalität für alle anderen Logdateien, denen diese Filterdatei zugeordnet ist. Falls Sie dies nicht wünschen, so müssen Sie das editierte Anzeigefilter unter einem neuen Namen speichern.

Der Filterdialog wird zusätzlich auch für den Pakettrigger benutzt. Dabei handelt es sich um ein Paketfilter, welches den Startzeitpunkt des Logprozesses festlegt. Solange kein Paket den Pakettrigger passiert, erfolgt auch keine Aufzeichnung. Nachdem schließlich ein Paket den Logvorgang 'triggert', wird der Pakettrigger deaktiviert und das Aufzeichnungsfiler beginnt stattdessen zu arbeiten. Das Triggerereignis wird durch das Verschwinden eines

kleinen grünen Punkts am Knopf **TR** der Werkzeugleiste angezeigt. Danach kann die Triggerfunktion jederzeit wieder durch Unterbrechen des Logs und Einschalten des Triggers reaktiviert werden. Beachten Sie außerdem, dass Sie Standarddateien für den Trigger sowie das Aufzeichnungs- und Anzeigefilter (in den LPA-Einstellungen, siehe Abschnitt 5.11) setzen können, welche dann immer automatisch nach dem Start der Software verwendet werden.

Das Aufzeichnungsfilters des aktiven Logs kann mittels [Menü Profile | Capture Filter...] oder Klick auf **CF** editiert werden. Das Anzeigefilter des aktuellen Logfensters kann mittels [Menü Profile | Display Filter...] oder Klick auf **DF** editiert werden. Ein kleiner grüner Punkt auf diesen Knöpfen zeigt an, dass das entsprechende Filter aktiviert ist. In Abbildung 37 ist das Dialogfenster für Paketfilter dargestellt.

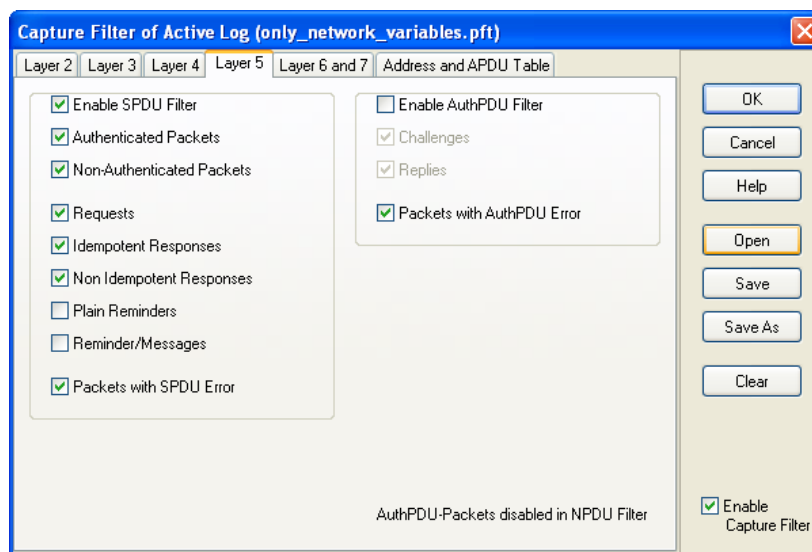


Abbildung 37: **Paketfilter**

Jedes Paketfilter ist gemäß den Schichten des Netzwerkprotokolls (Layer 2-7) in mehrere Sektionen aufgeteilt. Jede Sektion lässt sich (ganz oben) vollständig ein- und ausschalten ('Enable ...'). Wenn eine Filtersektion ausgeschaltet ist, wird auf der entsprechenden Protokollschicht nicht gefiltert. Es ist auch möglich, dass - aufgrund von Einstellungen in tieferen Protokollschichten des Filters - Teile des Filters automatisch deaktiviert werden. Falls dies zutrifft, erscheint eine entsprechende Nachricht im unteren Bereich der betroffenen Filtersektion. Abbildung 37 zeigt als Beispiel die Filtersektion für die Protokollschicht 5. In diesem Fall hat der Anwender das SPDU-Filter eingeschaltet und eingestellt, dass 'Non-Idempotent Responses' sowie 'Plain Reminders' verworfen werden sollen. Zum Zweck des höheren Datendurchsatzes oder falls alle Pakete angezeigt werden sollen, können Sie auch das gesamte Paketfilter mittels des 'Enable'-Felds (rechts unten) deaktivieren. Mit dem 'Clear'-Knopf können Sie den Standardfilter wiederherstellen, welcher alle fehlerhaften Pakete verwirft und alle korrekten Pakete durchlässt.

Address and APDU Table

Zusätzlich zu den protokollschichtspezifischen Filtersektionen existiert noch die Adress- und APDU-Tabelle für paketabsender- und -empfängerspezifische Einstellungen. Dies ist deshalb als separate Tabelle ausgeführt, da es sich dabei um eine Kombination aus Protokollschicht 3 (Netzwerkadressen) und den Schichten 6&7 (APDU) handelt. Abbildung 38 zeigt nochmals den Filterdialog, diesmal mit aktivierter Adress- und APDU-Tabelle.

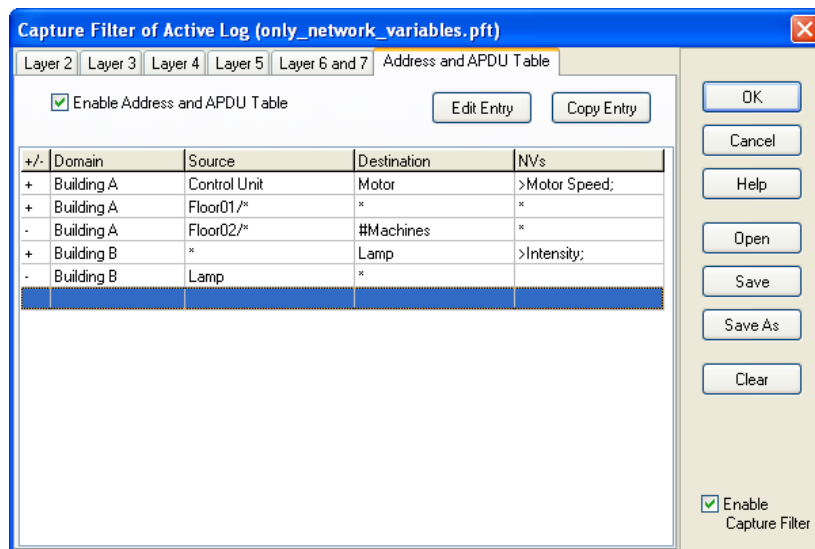


Abbildung 38: Adress- und APDU-Tabelle

Die erste Spalte jeder Zeile ('+/-') gibt an, ob es sich um einen positiven oder einen negativen Adresseintrag handelt. Ein Paket muss mindestens zu einem positiven Adresseintrag passen, darf jedoch zu keinem der negativen Einträge passen, um das Filter zu passieren. Deshalb muss auch immer mindestens ein positiver Eintrag existieren, da sonst überhaupt keine Pakete passieren könnten.

Einzelne Zeilen der Tabelle können mittels der Tasten ENTF und EINFG gelöscht bzw. eingefügt werden. Einen bestimmter Tabelleneintrag können Sie durch Klick auf 'Edit Entry' oder Doppelklick in die entsprechende Zeile editieren. Sie können auch einen Eintrag mittels 'Copy Entry' kopieren. In beiden Fällen wird der Adresseditor des Paketfilters aufgerufen, siehe Abbildung 39.

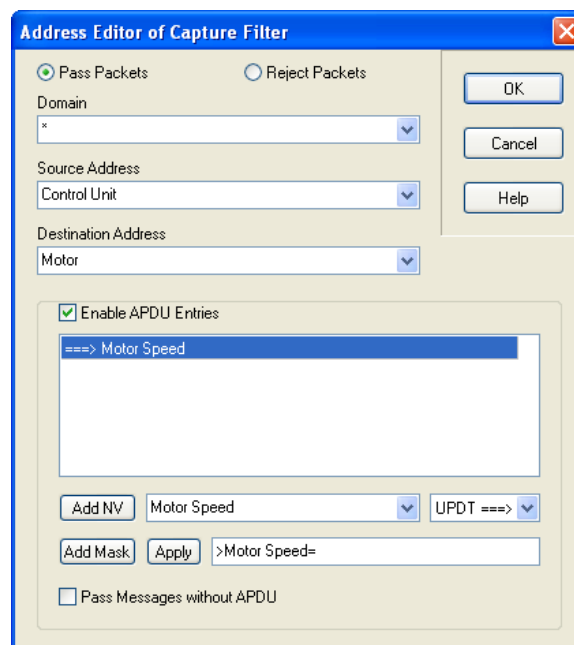


Abbildung 39: Adresseditor

Zunächst müssen Sie entscheiden, ob es sich um einen positiven ('Pass Packets') oder negativen ('Reject Packets') Eintrag handeln soll. Im 'Domain'-Feld können Sie einen symbolischen Domain-Namen aus dem Paketkonverter oder eine hexadezimale Domain-ID

eingeben. Falls Sie hier ein Sternzeichen (‘*’) eingeben, bedeutet dies ‘Alle Domains’. Im ‘Source Address’-Feld geben Sie den (die) zulässigen Absender des Pakets an. Folgende Eingabeformate sind zulässig:

- * ... Absenderadresse wird nicht überprüft,
- 0/0 ... Absender ist unkonfiguriert,
- Subnet/* ... alle Absender dieses Subnets,
- Subnet/Knotennummer ... nur Pakete mit dieser Absenderadresse,
- Knotenname ... Absender muss der spezifizierte Knoten sein.

Das ‘Destination Address’-Feld spezifiziert den (die) zulässigen Empfänger des Pakets. Folgende Eingabeformate sind zulässig:

- * ... Empfängeradresse wird nicht überprüft,
- 0/* ... alle domain-weiten Broadcasts,
- Subnet/* ... alle Empfänger dieses Subnets,
- Subnet/Knotennummer ... nur Pakete mit dieser Empfängeradresse,
- #Gruppe ... Pakete mit dieser Gruppe als Empfängeradresse,
- NID ... Pakete mit dieser NID als Empfängeradresse,
- Knotenname ... Der spezifizierte Knoten muss (einer) der Empfänger sein.

Beachten Sie, dass Sie neben dezimalen und hexadezimalen Zahlen auch symbolische Namen aus dem Paketkonverter für Subnets und Gruppen verwenden können. Wenn Sie einen symbolischen Knotennamen als Empfängeradresse benutzen, passt jedes Paket zu diesem Adresseintrag, welches den angegebenen Knoten adressiert, unabhängig vom Adressformat des Pakets. Sie haben z.B. den Knoten ‘Lamp1’ im Paketkonverter mit der NID 0x001122334455 in der Domain 0x00 mit Subnet/KnotenNr 1/1 und den Gruppen 0, 1 & 2 eingegeben. Wenn Sie dann im Adresseditor, wie oben gezeigt, ‘Lamp1’ als ‘Destination Address’ spezifizieren, so passen folgende Pakete zu diesem Eintrag:

- Broadcasts in Domain 0x00,
- Broadcasts in Subnet 1 der Domain 0x00,
- Pakete mit Empfänger-Subnet/Knotennummer 1/1 in Domain 0x00,
- Pakete der Gruppe 0, 1 oder 2 in Domain 0x00,
- Pakete mit Empfänger-NID 0x001122334455.

Sollten Sie, wie zu Beginn beschrieben, das Sternzeichen (‘*’) im ‘Domain’-Feld eingegeben haben, können Sie jeden im Konverter eingegebenen Knoten als ‘Destination Address’ auswählen (unabhängig von seinen Domain-Tabellen, was auch unkonfigurierte Knoten einschließt). In diesem Fall können allerdings nur Pakete mit NID als Empfängeradresse den Adresseintrag passieren und somit wäre lediglich der letzte Punkt des obigen Beispiels gültig.

APDU Entries

Hier können Sie Filterkriterien basierend auf dem Applikationsteil der Pakete (APDU) spezifizieren. Folgende Filtermethoden werden dabei unterstützt:

1. Filtern auf Netzwerkvariablen (Polls, Updates) ohne Datenvergleich

Geben Sie dazu einfach die gewünschte Netzwerkvariable neben dem 'Add NV'-Knopf ein und drücken dann auf 'Add NV'. Eine Netzwerkvariable kann als symbolischer Netzwerkvariablenname (aus einem Knoten des Paketkonverters) sowie als Selektor in dezimaler (z.B.: 12345) oder hexadezimaler (z.B.: 0x0ABC) Form eingegeben werden. Zuvor können Sie die Richtung der Variable einstellen ('UPDaTe', 'POLL' oder 'BOTH').

2. Filtern auf Netzwerkvariablen-Updates mit Datenvergleich

Geben Sie eine Zeile folgenden Formats in das Feld neben dem 'Apply'-Knopf ein:

- >Netzwerkvariable= Datenmaske

und klicken Sie auf 'Add Mask'. Alle Updates dieser Netzwerkvariable, deren (aktualisierter) Wert der Datenmaske entspricht, können dann diesen Eintrag passieren. Die Bytes der Maske können entweder hexadezimal (z.B.: "10 0A C7") oder binär (mit vorangestelltem Punkt, z.B.: ".00101011") eingegeben werden. Als Wildcard kann das "?" verwendet werden, um bestimmte Nibbles oder Bits zu ignorieren (z.B.: "?5 ?? F? " oder ".01?00??1").


3. Generisches Filtern der APDU

Geben Sie dazu einfach eine Datenmaske für die komplette APDU in das Feld neben dem 'Apply'-Knopf ein und klicken Sie dann auf 'Add Mask'. Im Folgenden sind einige Beispiele angeführt:

- 20 ... alle Application Msgs. mit Msg.Code 0x20
- 20 12 .11110000 ... alle Appl. Msgs. mit Msg.Code 0x20 und Datenbytes 0x12 0xF0
- 2? ... alle Application Msgs. mit Msg.Codes 0x20 - 0x2F
- .1??????? .???????? ... alle Netzwerkvariablen Msgs. (2 Bytes Msg.Code, MSB=1)
- 6A ... alle Query Domain Msgs. (Netzwerkmanagement Code 0x6A)
- 40 ?? ?? ... alle Foreign Frame Msgs. mit MsgCode 0x40 und mindestens 2 Datenbytes
- 10 .1??????? ... alle Appl. Msgs. mit MsgCode 0x10 und MSB=1 im 1. Datenbyte
- 10 ?? AB ... alle Application Msgs. mit Msg.Code 0x10 und 2. Datenbyte = 0xAB

Um eine existierende Maske zu ändern, klicken Sie auf die entsprechende Zeile, editieren Sie die Maske und klicken schließlich auf 'Apply'. Um einen APDU-Eintrag zu löschen, klicken Sie auf die entsprechende Zeile und drücken Sie ENTF. Um auch Pakete ohne APDU passieren zu lassen, aktivieren Sie das Feld ganz unten ('Pass Messages without APDU').

5.4 Anzeigeeoptionen

Jedem Logfenster sind Anzeigeeoptionen zugeordnet, wodurch die Darstellung bestimmter Spalten der Pakettabelle konfiguriert werden kann. Die Anzeigeeoptionen des aktuellen Logfensters können mittels [Menü View | Display Options...], Klick auf den Knopf  sowie des Kontextmenüs (siehe Abschnitt 4.6) aufgerufen werden. Abbildung 40 zeigt das entsprechende Dialogfenster.

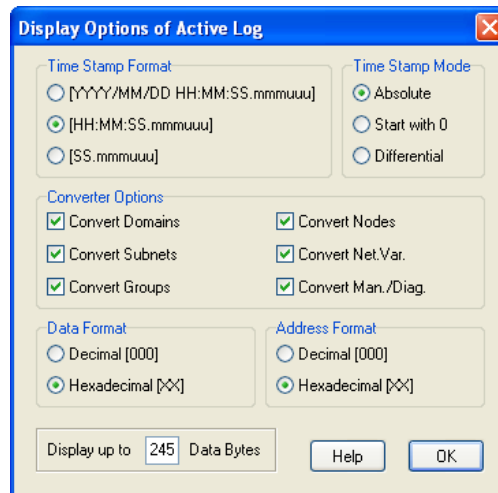


Abbildung 40: Anzeigeeoptionen

Time Stamp Format

Hier können Sie das Format des Zeitstempels einstellen.

Time Stamp Mode

Hier können Sie zwischen drei Anzeigemodi für den Zeitstempel wählen: ‘Absolute’ bedeutet, dass die tatsächliche Empfangszeit des Pakets angezeigt wird. ‘Start with 0’ bedeutet, dass die Differenz zwischen erstem und aktuellem Paket angezeigt wird. Wenn Sie ‘Differential’ wählen, wird die Zeit zwischen dem jeweils vorhergehenden und dem aktuellen Paket angezeigt.

Converter Options

Hier können Sie die Übersetzung von Domains, Subnets, Gruppen, Knoten, Netzwerkvariablen sowie Management- und -diagnosenachrichten ausschalten. Standardmäßig werden diese Übersetzungen (von den Zahlen im Paket zu symbolischen Namen) automatisch mittels des Paketconverters vorgenommen.

Data Format

Hier können Sie das Format (dezimal oder hexadezimal) der Nachrichtendaten in der Pakettabelle einstellen. Diese Einstellung beeinflusst auch die Anzeige der Daten in den Paket- und Protokolldetails des Logfensters.

Address Format


Hier können Sie das Format der unkonvertierten Adressinformation (Subnet-ID, Guppen-ID, Knotennummer) in den Spalten Absenderadresse (Source) und Empfängeradresse (Destination) einstellen. Diese Einstellung beeinflusst auch die Anzeige der Adressen in den Paketdetails. In den Protokolldetails des Logfensters hingegen werden Adressen immer in

hexadezimaler und dezimaler Form dargestellt. Beachten Sie außerdem, dass Domain-IDs und NIDs grundsätzlich immer hexadezimal angezeigt werden.

Display up to ... Data Bytes

Hier können Sie die Anzahl an Datenbytes (bis zu 245) einstellen, die in der Datenspalte der Pakettabelle angezeigt werden sollen. Wenn im Paket mehr Datenbytes enthalten sind, werden diese nicht dargestellt. In den Protokolldetails des Logfensters können Sie jedoch immer die gesamten Daten eines Pakets sehen, unabhängig von der hier erläuterten Einstellung.

5.5 Paketstatistik

Das Paketstatistikfenster, welches mittels [Menü Packet | Statistics] oder Klick auf den Knopf  aufgerufen wird, zeigt die Statistikdaten des aktuellen Logfensters, siehe Abbildung 41 (links). Es kann ebenfalls für den aktiven Log während des Logprozesses eingeblendet werden, falls diese Option in den Logmoduseinstellungen aktiviert ist. Für diesen Fall befindet sich in der rechten oberen Ecke des Fensters ein 'Clear'-Knopf, mit dem man jederzeit die Statistikdaten rücksetzen kann, siehe Abbildung 41 (rechts).

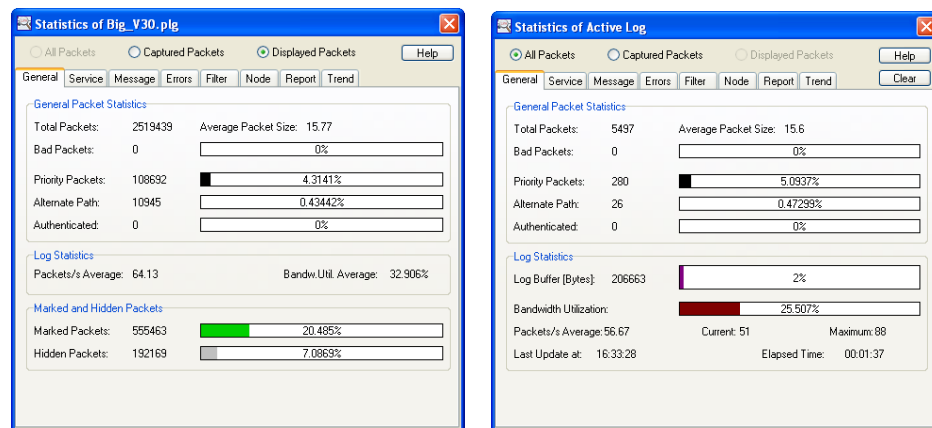


Abbildung 41: **Paketstatistik für normales Logfenster und Aktiven Log**

Ganz oben im Statistikfenster kann eingestellt werden, ob die Statistik über alle Pakete oder nur jene, die den entsprechenden Paketfilter passiert haben, berechnet werden soll. Für den aktiven Log ist hiermit das Aufzeichnungsfiler, für alle anderen Logfenster das Anzeigefilter gemeint. Deshalb kann im ersten Fall auch zwischen 'All Packets' (alle Pakete) und 'Captured Packets' (aufgezeichnete Pakete), im zweiten Fall hingegen zwischen 'Captured Packets' und 'Displayed Packets' (angezeigte Pakete) gewählt werden. Weitere Unterschiede zwischen der Statistik für bereits fertig aufgezeichnete Logdateien und jener für den aktiven Log werden weiter unten beschrieben. Beachten Sie, dass die Anzahl der aufgezeichneten Pakete auch jederzeit der Statusleiste entnommen werden kann. Das Paketstatistikfenster ist in mehrere Sektionen unterteilt:

General

In der 'General Packet Statistics'-Sektion werden die absolute Anzahl der Pakete, die durchschnittliche Paketlänge sowie die Zahl der fehlerhaften Pakete ('Bad Packets') angezeigt. Bei den korrekten Paketen wird angezeigt, wieviele davon Priority-, Alternate-Path- oder Authenticated-Pakete sind. Im unteren Bereich können Sie entweder die Untersektion 'Log Statistics' (bei der Statistik des aktiven Logs) oder die beiden Untersektionen 'Log Statistics' und 'Marked and Hidden Packets' (bei normalen Logfenstern) sehen. Im ersten Fall wird der Zustand des Logpuffers sowie die Bandbreitenausnutzung ('Bandwidth Utilization') und der Paketdurchsatz ('Packets/s')

angezeigt, im zweiten Fall die Zahl der markierten und ausgeblendeten Pakete (siehe Abschnitt 4.6). Die Bandbreitenausnutzung wird aus den Paketlängen (inklusive Preamble, Startbit & Code-Violation) sowie den durchschnittlichen Arbitrationszeiten zwischen den Paketen (β_1 -Zeit, β_2 -Slots) berechnet. Eine Bandbreitenausnutzung von 100% würde bedeuten, dass kontinuierlich Pakete gesendet werden, ohne ungenutzte Wartezeit zwischen den Paketen.

Service

Hier wird angezeigt, wieviele der korrekten Pakete TPDU-, SPDU-, AuthPDU- oder Unacknowledged-Pakete sind. Für jedes der genannten PDU-Formate existiert außerdem noch eine genauere Unterteilung in bestimmte Services.

Message

In dieser Sektion werden die korrekten Pakete gemäß ihres Nachrichtentyps (APDU-Type) unterteilt.

Errors

Im 'Bad Packets'-Feld wird die Zahl der fehlerhaften Pakete (Pakete mit Protokollfehler) jeder Protokollschicht einschließlich zu kurzer und zu langer Pakete angezeigt. Kurze Pakete ('Short Packets') können durch Störungen am Netzwerk sowie Kollisionen während der Aussendung der Adressinformation entstehen. Der CRC-Fehlerzähler wird erhöht, wenn Pakete mit fehlerhaftem CRC empfangen werden. CRC-Fehler können ebenfalls durch Störungen am Netzwerk oder Kollisionen (z.B. im Datenbereich des Pakets) hervorgerufen werden. Alle anderen Zähler des 'Bad Packets'-Felds zeigen ungültige Werte der zu den entsprechenden Protokollschichten 3-7 gehörigen Paketinformationen an.

Im 'Error Counters'-Feld sehen Sie die absolute Fehlerzahl, einschließlich aller Fehler, welche nicht mit empfangenen Paketen assoziiert sind. Der 'Missed Preambles'-Fehlerzähler wird erhöht, wenn ein Paketfehler am Paketbeginn detektiert wurde. Der 'Interrupted Packets'-Zähler wird erhöht, wenn ein Paket im Bereich der Adressinformation unterbrochen wurde. Dies beinhaltet sowohl kurze Pakete ('Short Packets'), welche vom LPA aufgezeichnet wurden, als auch alle Pakete, welche zu kurz sind, um im Log gespeichert zu werden (kleiner 2 Bytes). Der 'Corrupted Packets'-Zähler wird erhöht, wenn ein korruptes Paket (oder Paketeil) detektiert wurde. Dies beinhaltet aufgezeichnete Pakete mit CRC-Fehler sowie CRC-Fehler in Paketen, welche zu kurz für die Aufzeichnung sind. Mögliche Ursachen für die beschriebenen Fehler sind: Kollisionen (mehrere Knoten versuchen zur selben Zeit zu senden), mangelhafte Verkabelung, zu hohes Kanalrauschen oder Einstreuungen von externen Geräten.

Verlorene Pakete ('Lost Packets') sollten normalerweise nicht auftreten, da aktuelle PCs schnell genug sind, um mit den typischen Paketraten von CEA-709-Netzwerken Schritt zu halten. Sollten Sie trotzdem Pakete verlieren, können Sie folgende Schritte befolgen, um den Paketdurchsatz Ihres LPAs zu erhöhen:

- Schließen Sie andere Applikationen.
- Löschen Sie den Paketkonverter.
- Deaktivieren Sie die Paketfilter (Aufzeichnungs- und Anzeigefilter).
- Ändern Sie den Logmodus (Deaktivieren des On-line-Modus).
- Deaktivieren Sie den LPA-Server und das LPA-Plug-In in den LPA-Einstellungen.

Filter

Hier können Sie sehen, wie viele Pakete auf jeder Protokollschicht gefiltert wurden. Die angezeigten Werte gelten für das Aufzeichnungsfiler, falls die Statistik des aktiven Logs angezeigt wird. Ansonsten gelten die Werte für das Anzeigefilter.

Die restlichen Sektionen des Statistikfensters ('Node', 'Report', and 'Trend') sind in den folgenden Abschnitten beschrieben.

Sie können die Aktualisierung des Paketstatistikfensters jederzeit mittels [Menü Packet | Pause Update] oder [Menü Packet | Pause Log] während des Logprozesses anhalten. Sie können jedoch auch dann durch Klick auf die Beschriftung der gerade sichtbaren Statistiksektion ('General', 'Service' ...) manuell eine Aktualisierung erzwingen.

5.6 Knotenstatistik

Die Knotenstatistik zeigt domain-, subnet-, knoten- und gruppenspezifische Statistikwerte. Sie wird mittels 'Node'-Reiter des Statistikfensters aufgerufen, wie in Abbildung 42 zu sehen ist.

The screenshot shows the 'Statistics of Big_V30.plg' window with the 'Node' tab selected. The window displays four tables: Domains, Subnets, Nodes, and Groups. The 'Node' table is selected, showing details for various nodes like '4A: Visualization', '0A: Zone Controller Beta', etc. The right sidebar contains controls for adjusting columns and filters.

Number	Domain	Subnets	Groups	Nodes	Senders	Receivers	Silent	Packets	Alt.Path
1	Building A	61	77	253	39	119	5	2305653	8399
2	Building B	27	4	253	3	232	1	405955	3232

Number	Domain	Subnet	Nodes	Senders	Receivers	Silent	Packets	Alt.Path
1	Building A	02: _Subnet_1_2	1	1	0	0	285744	6871
2	Building A	03: _Subnet_1_3	6	0	2	0	302450	16
3	Building A	05: _Subnet_1_5	2	0	0	0	6053	0
4	Building A	06: _Subnet_1_6	6	0	0	0	477274	8
5	Building A	07: _Subnet_1_7	2	0	0	0	5275	0

Number	Domain	Subnet	Node	Groups	Packets	Alt.Path	Type
1	Building A	02: _Subnet_1_2	4A: Visualization	0	285744	6871	Sender
2	Building A	03: _Subnet_1_3	0A: Zone Controller Beta	12	266340	0	Generic
3	Building A	03: _Subnet_1_3	33: Zone Controller Alpha	3	24257	8	Generic
4	Building A	03: _Subnet_1_3	37: Room Controller 3	0	650	0	Receiver
5	Building A	03: _Subnet_1_3	3A: Lighting 2	0	3453	8	Receiver
6	Building A	03: _Subnet_1_3	41: Heating Room 1	3	3305	0	Generic
7	Building A	03: _Subnet_1_3	4B: Heating Room 6	1	4445	0	Generic
8	Building A	05: _Subnet_1_5	21: Heating Room 4	1	3127	0	Generic
9	Building A	05: _Subnet_1_5	24: Heating Room 2	0	2926	0	Generic
10	Building A	06: _Subnet_1_6	09: Lighting 3	6	263441	0	Generic
11	Building A	06: _Subnet_1_6	08: Lighting 1	9	186324	0	Generic
12	Building A	06: _Subnet_1_6	18: Room Controller 1	1	4570	0	Generic
13	Building A	06: _Subnet_1_6	1F: Lighting 4	2	14110	0	Generic
14	Building A	06: _Subnet_1_6	24: Heating Room 5	2	4546	8	Generic
15	Building A	06: _Subnet_1_6	27: Heating Room 3	1	4283	0	Generic
16	Building A	07: _Subnet_1_7	0B: Room Controller 2	1	2642	0	Generic

Number	Domain	Group	Nodes	Packets	Alt.Path	Ackd
1	Building A	06	1	6782	0	0
2	Building A	09	1	8421	0	0
3	Building A	0F	5	18155	0	0
4	Building A	1E	1	28435	0	0
5	Building A	1F	1	32400	0	0

Abbildung 42: Knotenstatistik

Alle detektierten Domains, Subnets, Knoten und Gruppen werden in vier separaten Tabellen angezeigt. Wird eine bestimmte Zeile einer Tabelle angeklickt, so werden alle entsprechenden Zeilen der anderen Tabellen blau hinterlegt sowie mit einem Dreieck-Zeichen in der 'Number'-Spalte gekennzeichnet. In Abbildung 42 wird auf diese Weise z.B. angezeigt, dass sich der ausgewählte Knoten 'Lighting 1' in der Domain 'Building A' im

Subnet ‘_Subnet_1_6’ befindet und ein Mitglied der Gruppe 0x09 ist. Subnet- Knoten- und Gruppennummern werden dezimal oder hexadezimal angezeigt, entsprechend den aktuellen Anzeigeeoptionen des Logs, siehe Abschnitt 5.4. Die Tabellen können durch Anklicken der Spaltenüberschriften sortiert werden. Hierarchische Sortierung erfolgt mittels Anklicken verschiedener Spaltenüberschriften, beginnend mit der für die Sortierung niederwertigsten Spalte und endend bei der höchstwertigsten Spalte. Die Breite jeder Spalte kann durch Doppelklick auf den rechten Rand der Spaltenüberschrift den angezeigten Werten angepasst werden. Im Folgenden sind die Spalten aller Tabellen kurz beschrieben:

Tabelle ‘Domains’

Spalte ‘Domain’: Domainnummer oder -name (abhängig vom Paketkonverter),
Spalten ‘Subnets’, ‘Groups’, ‘Nodes’: Anzahl der Subnets, Gruppen, Knoten der Domain,
Spalte ‘Senders’: Anzahl der Knoten, die primär Transaktionen initiieren,
Spalte ‘Receivers’: Anzahl der Knoten, die primär auf initiierte Transaktionen antworten,
Spalte ‘Silent’: Anzahl der Knoten, die selbst keine Pakete senden (stumme Knoten),
Spalte ‘Packets’: Anzahl gesendeter Pakete in dieser Domain,
Spalte ‘Alt.Path’: Anzahl gesendeter Alternate-Path Pakete dieser Domain.

Tabelle ‘Subnets’

Spalte ‘Domain’: Domain, in welcher sich das Subnet befindet,
Spalte ‘Subnet’: Subnetnummer und -name (abhängig vom Paketkonverter),
Spalte ‘Nodes’: Anzahl der Knoten des Subnets,
Spalte ‘Senders’: Anzahl der Knoten, die primär Transaktionen initiieren,
Spalte ‘Receivers’: Anzahl der Knoten, die primär auf initiierte Transaktionen antworten,
Spalte ‘Silent’: Anzahl der Knoten, die selbst keine Pakete senden (stumme Knoten),
Spalte ‘Packets’: Anzahl gesendeter Pakete in diesem Subnet,
Spalte ‘Alt.Path’: Anzahl gesendeter Alternate-Path Pakete dieses Subnets.

Tabelle ‘Nodes’

Spalte ‘Domain’: Domain, in welcher sich der Knoten befindet,
Spalte ‘Subnet’: Subnet, in welchem sich der Knoten befindet,
Spalte ‘Node’: Knotennummer und -name (abhängig vom Paketkonverter),
Spalte ‘Groups’: Anzahl der Gruppen, für welche der Knoten als Mitglied detektiert wurde,
Spalte ‘Packets’: Anzahl der von diesem Knoten gesendeten Pakete,
Spalte ‘Alt.Path’: Anzahl der von diesem Knoten gesendeten Alternate-Path Pakete,
Spalte ‘Type’: ‘Sender’, ‘Receiver’, ‘Generic’ (kein spezifisches Sendeschema), ‘Silent’.

Tabelle ‘Groups’

Spalte ‘Domain’: Domain, in welcher sich die Gruppe befindet,
Spalte ‘Group’: Gruppennummer und -name (abhängig vom Paketkonverter),
Spalte ‘Nodes’: Anzahl der Knoten, welche als Mitglied dieser Gruppe detektiert wurden,
Spalte ‘Packets’: Anzahl gesendeter Pakete in dieser Gruppe,
Spalte ‘Alt.Path’: Anzahl gesendeter Alternate-Path Pakete dieser Gruppe,
Spalte ‘Ackd’: Anzahl der Pakete, welche mittels Acknowledged-Dienst gesendet wurden.

Alternate-Path Pakete werden generell immer dann gesendet, wenn der Empfängerknoten nicht antwortet. Die Anzahl von Alternate-Path Paketen - welche in allen vier Tabellen angezeigt wird - ist daher ein Anzeichen für Probleme mit (einem oder mehreren) Empfängerknoten. Stumme Knoten (‘Silent’) sollten ebenfalls untersucht werden, um festzustellen, warum die adressierten Knoten auf dem beobachteten Netzwerksegment nicht senden. Die Anzahl der Acknowledged Pakete in Gruppen (letzte Spalte) wird angezeigt, da es mit diesem Dienst zu Problemen in größeren Gruppen kommen kann. Detaillierte Informationen über alle detektierten Netzwerkprobleme können dem LPA-Report entnommen werden, siehe Abschnitt 5.7.

Im rechten Teil des Knotenstatistikfensters sind folgende Optionen und Funktionen verfügbar:

Adjust Columns

Passt die Breite aller Spalten den angezeigten Werten an.

Default Address Sort

Sortiert alle Tabellen hierarchisch nach der Adresse (z.B. nach Domain / Subnet / Knoten im Fall der Knotentabelle).

Total Packet Counts

Dient der Einstellung des Anzeigemodus der 'Packets'-Spalten aller vier Tabellen. 'Absolute' zeigt die absolute Paketanzahl, '% of Traffic' zeigt die relative Paketanzahl bezogen auf den Gesamtverkehr, 'Average Rate' zeigt die durchschnittliche Paketrate und 'Current Rate' die aktuelle Paketrate (nur on-line verfügbar).

Alt.Path Packets

Dient der Einstellung des Anzeigemodus der 'Alt.Path'-Spalten aller vier Tabellen. 'Absolute' zeigt die absolute Anzahl von Alternate-Path Paketen, '% of Total' zeigt die relative Anzahl bezogen auf die absolute Paketanzahl der Domain, des Subnets, des Knotens oder der Gruppe.

Ackd Packets

Dient der Einstellung des Anzeigemodus der 'Ackd'-Spalte der Gruppentabelle. 'Absolute' zeigt die absolute Anzahl von Paketen mit Acknowledged-Dienst, '% of Total' zeigt die relative Anzahl bezogen auf die absolute Paketanzahl der Gruppe.

Show S/N/G No.

Wenn diese Option aktiviert ist, werden Subnet-, Knoten- und Gruppennummern in jedem Fall angezeigt, selbst wenn symbolische Namen im Paketkonverter verfügbar sind, siehe z.B. die Spalten 'Subnet' und 'Node' in der Knotentabelle der Abbildung Abbildung 42. Wenn die Option deaktiviert ist, erfolgt eine numerische Darstellung ausschließlich dann, wenn keine symbolischen Namen verfügbar sind. Beachten Sie, dass in diesem Fall die entsprechenden Spalten nach Namen sortiert werden.

Enable Disp. Filter

Diese Checkbox kann verwendet werden, um ein Anzeigefilter wieder zu deaktivieren, welches zuvor automatisch mittels einer der folgenden zwei Funktionen generiert wurde:

Create Display Filter

Klicken Sie auf diesen Knopf, um ein Anzeigefilter zu erzeugen, welches ausschließlich Pakete des aktuell ausgewählten Elements (Domain, Subnet, Knoten oder Gruppe) anzeigt. Sollte ein Knoten ausgewählt sein, so werden sowohl gesendete *als auch empfangene* Pakete dieses Knoten angezeigt, so sie dem Knoten zugeordnet werden können.

Add to Display Filter

Klicken Sie auf diesen Knopf, um das aktuell ausgewählte Element (Domain, Subnet, Knoten oder Gruppe) einem bereits existierenden Anzeigefilter hinzuzufügen. Auf diese Weise kann z.B. der Verkehr mehrerer Knoten angezeigt werden.

Converter Entry...

Klicken Sie auf diesen Knopf, um den Paketkonvertiereintrag des ausgewählten Elements (Domain, Subnet, Knoten oder Gruppe) zu erstellen bzw. zu ändern.

Export Table...

Klicken Sie auf diesen Knopf, um die aktuell ausgewählte Tabelle als CSV-Datei (Comma Separated Value) zu exportieren. Die entsprechenden Trennzeichen können in den LPA-Einstellungen ausgewählt werden (Abschnitt 5.11).

Beachten Sie, dass die fünf letztgenannten Funktionen auch über das Kontextmenü der Domain-, Subnet-, Knoten- und Gruppentabelle verfügbar sind, siehe Abbildung 43.

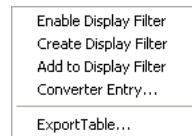


Abbildung 43: Kontextmenü der Knotenstatistik

5.7 LPA-Reports

LPA-Reports bieten eine rasche Übersicht über das beobachtete Netzwerksegment. Der Report-Abschnitt des Statistikfensters ist in Abbildung 44 zu sehen.

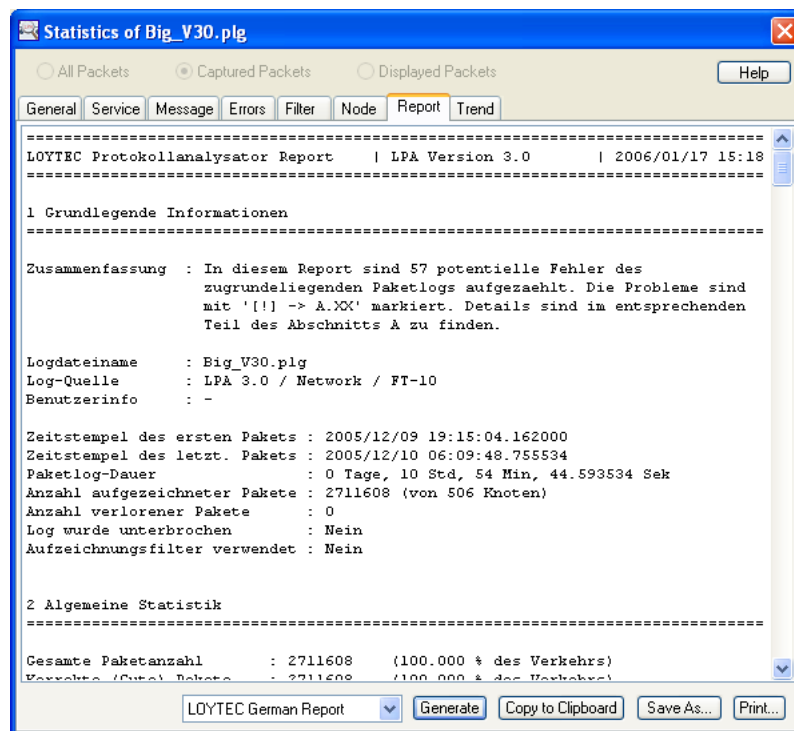


Abbildung 44: LPA-Report

Im unteren Teil des Fensters kann die Reportvorlage ausgewählt werden, bevor der Report mittels 'Generate' erstellt wird. Es besteht die Möglichkeit, kundenspezifische Reportvorlagen zu programmieren, siehe Abschnitt 6.4. Der Report kann in die Zwischenablage kopiert ('Copy to Clipboard') und danach in verschiedene Applikationen eingefügt werden. Er kann außerdem gespeichert ('Save As...') sowie gedruckt ('Print...')

werden. Die Reportdateien, welche mittels LOYTEC Reportvorlagen erstellt werden, bestehen aus den folgenden Abschnitten:

1 Grundlegende Informationen

Beinhaltet grundlegende Informationen über die analysierte Logdatei und bietet eine kurze Zusammenfassung der Probleme.

2 Allgemeine Statistik

Zeigt allgemeine Paketstatistiken entsprechend den verschiedenen Protokollschichten.

3 Fehlerstatistik

Beinhaltet die wichtigsten Zähler für fehlerhafte Pakete sowie weitere Fehlerzähler einschließlich einer kurzen Beschreibung der gezeigten Werte.

4 Domain-Statistik

Zeigt allgemeine Statistikwerte aller detektierten Domains. Die Domains werden dabei wie in der Knotenstatistik sortiert.

5 Potentielle Knotenprobleme

Zählt alle potentiellen Knotenprobleme, wie Alternate-Path Pakete oder stumme Knoten auf. Die gezeigten Knoten werden dabei wie in der Knotenstatistik sortiert.

6 Potentielle Probleme mit Gruppen

Zählt alle potentiellen Probleme mit Gruppen auf. Die gezeigten Gruppen werden dabei wie in der Knotenstatistik sortiert.

A Anhang

Bietet eine detaillierte Beschreibung aller detektierten Probleme einschließlich Hinweise zur Problemlösung.

5.8 Statistiktrend

Im Trend-Abschnitt des Statistikfensters wird der zeitliche Verlauf (Trend) der Bandbreitenauslastung sowie der Fehlerzähler für Missed Preambles und korrupte Pakete angezeigt, wie in Abbildung 45 zu sehen ist.

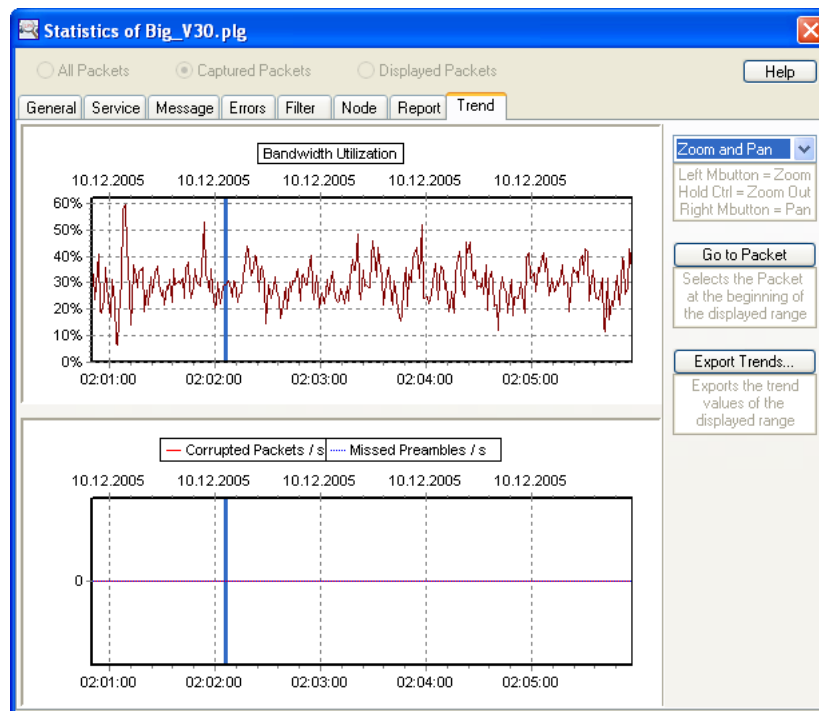


Abbildung 45: Statistiktrend

Beachten Sie, dass der Trend nur für Paketlogs verfügbar ist, welche mit LPA 3.0 oder höher generiert wurden. Sie können mittels Links-Klick in den Trend hineinzoomen. Durch Drücken der STRG-Taste und gleichzeitigem Links-Klick können Sie hinauszoomen. Weiters können Sie den betrachteten Abschnitt mittels Rechts-Klicken und Ziehen verschieben. Der rechte Teil des Trendfensters bietet außerdem folgende Funktionen:

Zoom Auswahl-Box (rechts oben)

Hier können Sie zwischen verschiedenen Zoom-Levels wählen: 'Show All' zeigt den gesamten Trend. 'Zoom and Pan' erlaubt das freie Zoomen und Verschieben des Ausschnitts, wie oben beschrieben. Alle weiteren Optionen zeigen einen bestimmten Ausschnitt am Ende des Trends. Dies ist vor allem im On-line-Betrieb hilfreich, da in diesem Fall die Diagramme automatisch nach links scrollen, sobald neue Werte eintreffen.

Go to Packet (nur off-line verfügbar)

Klicken Sie auf diesen Knopf, um das Paket am Beginn des aktuell dargestellten Trendausschnitts anzuspringen (auszuwählen). Die Position des aktuell ausgewählten Pakets ist immer als blauer Balken in den Trenddiagrammen sichtbar, siehe Abbildung 45.

Export Trends... (nur off-line verfügbar)

Klicken Sie auf diesen Knopf, um alle Trendwerte als CSV-Datei (Comma Separated Value) zu exportieren. Die entsprechenden Trennzeichen können in den LPA-Einstellungen ausgewählt werden (Abschnitt 5.11).

5.9 Paketsimulation

Um mehr über die Funktionen der LPA-Software sowie das Netzwerkprotokoll zu lernen, können Sie Pakete simulieren, als ob diese von einem real existierenden Netzwerk stammen würden. Jedes mögliche korrekte aber auch fehlerhafte Paket kann mittels Ihrer Eingabe erzeugt werden. Alle Funktionen des Analysators wie Filtrierung, Konversion und Statistik

können während der Simulation genutzt werden. Nachdem Sie einen neuen aktiven Log erzeugt und den Logmodus eingestellt haben, können Sie die Paketsimulation über [Menü Packet | Start Log | Simulate] starten. Daraufhin erscheint ein entsprechendes Dialogfenster, siehe Abbildung 46.

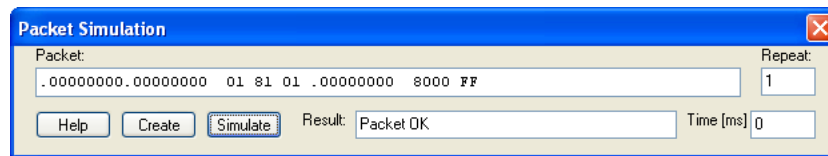


Abbildung 46: Paketsimulation

Hier können Sie Pakete simulieren, als ob sie von einem real existierenden Netzwerk kommen würden. Sie können das Paket in Rohform im Feld 'Packet:' eingeben. Beachten Sie, dass der CRC automatisch berechnet wird und daher nicht eingegeben werden muss. Paketbytes können sowohl hexadezimal (z.B.: 'FF 0A C7') als auch binär (mit vorangestelltem Punkt, z.B.: '.00101011') eingegeben werden. Sie können das Paket außerdem durch entsprechende Angabe im Feld 'Repeat:' wiederholt hintereinander senden. Nach der simulierten Aussendung des Pakets (bzw. der Pakete) durch Klick auf 'Simulate' erscheint im Feld 'Result:' eine Meldung, welche über Protokollfehler sowie eventuelle Abweisung durch den Pakettrigger, das Aufzeichnungsfilter oder das Anzeigefilter Auskunft gibt. Außerdem wird im Feld 'Time' die Zeitspanne der simulierten Aussendung angezeigt, was eine ungefähre Aussage über den Paketdurchsatz des LPAs auf Ihrem PC zulässt. Wenn Sie das Paket auf funktioneller Ebene zusammenstellen wollen, können Sie dazu mittels 'Create' das Paketerzeugungsfenster aufrufen, siehe Abbildung 47.

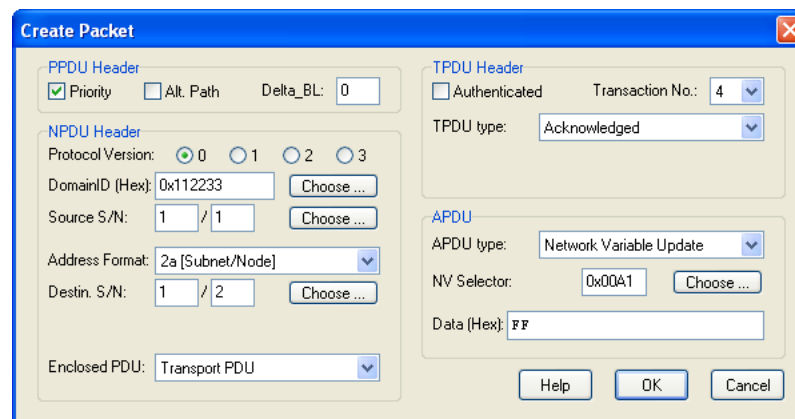


Abbildung 47: Paketerzeugung

Hier können Sie alle Parameter, welche zur Paketzusammenstellung nötig sind, eingeben. Dies beginnt bei Schicht 2 (erstes Paketbyte) und endet auf Schicht 6&7 des Netzwerkprotokolls. Auf diese Weise können Sie sich unter anderem mit den verschiedenen Paketformaten vertraut machen. Beachten Sie, dass hier nur korrekte Pakete (ohne Protokollfehler) erzeugt werden können; sollten Sie absichtlich Protokollfehler einbauen wollen, so müssen Sie dies anschließend manuell im Simulatorfenster tun. Das Paketerzeugungsfenster besteht aus folgenden Feldern:

PPDU Header

Dies repräsentiert Schicht 2 des Netzwerkprotokolls. Hier können Sie das Priority- und Alternate-Path-Flag sowie die Channel-Delta-Backlog ('Delta_BL') setzen.

NPDU Header

Die Network-PDU (Protocol Data Unit) repräsentiert Schicht 3 des Netzwerkprotokolls. Hier können Sie die Protokollversion, Adressinformationen und das transportierte PDU-Format ('Enclosed PDU') konfigurieren. Zunächst geben Sie die Domain-ID sowie das Absender-Subnet und die Absenderknotennummer ein ('Source S/N'). Für die Empfängeradresse müssen Sie zuerst das Adressformat wählen. Je nach Format müssen Sie dann die Empfänger-Subnet-ID, -knotennummer, -gruppe oder -NID eingeben. Im Adressformat 2b müssen Sie zusätzlich noch die Absendergruppe und -mitgliedsnummer ('Source G/M') eingeben. Sie können alle Adressinformationen auch automatisch, durch Wahl eines symbolischen Namens aus dem Paketkonverter (mittels Klick auf entsprechenden 'Choose...'-Knopf), einstellen.

TPDU, SPDU oder AuthPDU Header

Dies ist die Sektion im oberen, rechten Bereich des Fensters. Je nach Einstellung im NPDU-Header ('Enclosed PDU') erscheint dort einer der drei Header. Die Sektion repräsentiert Schicht 4 bzw. 5 des Netzwerkprotokolls. Hier können Sie das Authenticated-Flag und die Transaktionsnummer des Pakets setzen. Jeder der drei möglichen Header (TPDU, SPDU oder AuthPDU) bietet verschiedene Services, welche im Feld '...PDU type:' ausgewählt werden können. Einige der Services verlangen nach Zusatzinformationen (Member-List, Random-Bytes, Crypto-Bytes), welche hexadezimal am unteren Ende der Sektion eingegeben werden müssen.

APDU

Die APDU-Sektion erscheint, wenn Nachrichtendaten (Application Protocol Data Unit) im ausgewählten Paketformat transportiert werden können. In Acknowledgements, Plain-Reminders, Challenges und Replies kann keine APDU transportiert werden. In allen anderen Fällen müssen Sie zunächst den APDU-Typ wählen. Wenn Sie 'Network Variable Update' oder 'Network Variable Poll' wählen, so müssen Sie zusätzlich den entsprechenden Netzwerkvariablenelektor eingeben ('NV Selector:'). Ansonsten müssen Sie den gewünschten Message-Code ('... Code:') eingeben. Das Selektor- oder Code-Feld kann auch automatisch durch Wahl eines symbolischen Netzwerkvariablen- oder Message-Namens (mittels 'Choose...') gesetzt werden. Wollen Sie keine Nachrichtendaten im Paket transportieren, so wählen Sie 'APDU with Length 0'. Ansonsten können Sie schließlich die gewünschten Daten in hexadezimaler Form im Feld 'Data (Hex)' eingeben.

Wenn Sie auf 'OK' klicken, wird das Paket zusammengestellt und in das 'Packet:'-Feld des Simulationsfensters geschrieben (siehe Abbildung 46).

5.10 Packet-Recording-Dateien

Bei Packet-Recording-Dateien handelt es sich um Binärdateien, in welchen alle eintreffenden Pakete während eines Logprozesses gespeichert werden. Sie besitzen die Endung '.prc'. Um eine Packet-Recording-Datei zu erzeugen, wählen Sie 'Wrap Around Buffer and Record to File:' in den Logmoduseinstellungen [Menü Profile | Log Mode...] und starten den Log über [Menü Packet | Start Log]. Alle empfangenen Pakete werden dann direkt in die Packet-Recording-Datei geschrieben. Der Vorteil dieser Methode ist, dass Sie Pakete aufzeichnen können, solange Platz auf Ihrer Festplatte vorhanden ist (bis maximal 16 GB). Normale Logdateien können hingegen nur soviel Pakete aufnehmen, als in den Hauptspeicher passen (bis maximal 128 MB). Der Nachteil ist, dass Sie eine Packet-Recording-Datei nicht direkt öffnen können, Sie müssen stattdessen einen neuen Log aus der Datei starten.

Pakete können in zwei Modi aus einer Packet-Recording-Datei (oder Logdatei) geloggt werden: Standardmodus [Menü Packet | Start Log | from File...] und Trace-Modus [Menü

Packet | Start Log | from File (trace)...]. Im Standardmodus werden die Pakete so schnell als möglich aus der Datei geloggt; die Zeitstempel der Pakete bleiben dabei unverändert. Wenn Sie den Log im Trace-Modus starten, werden die Pakete so simuliert, als ob sie von einem realen Netzwerk kommen würden, mit einer Verzögerung von ca. 2 Sekunden zwischen aufeinanderfolgenden Paketen. Der Zeitstempel jedes Pakets wird in diesem Fall auf die 'Empfangszeit' im neuen Logpuffer gesetzt. Auf diese Weise können Packet-Recording-Dateien nicht nur für die Langzeitaufzeichnung sondern auch für Demonstrationszwecke, den LPA und das Netzwerkprotokoll betreffend, verwendet werden (siehe auch Kapitel 3). Beachten Sie, dass im Trace-Modus alle Funktionen des LPAs verfügbar sind, genauso, als würden Sie von einem realen Netzwerk aufzeichnen.

Um möglichst flexibel zwischen Logdateien und Packet-Recording-Dateien wechseln zu können, kann auch eine Logdatei als Quelle eines neuen Logs dienen. Ebenfalls ist es möglich, *von* einer Packet-Recording-Datei *in* eine neue zu loggen. Dies kann zur Datenreduktion mittels Filtrierung unerwünschter Pakete (bei Einsatz eines Aufzeichnungsfilters) verwendet werden. Zusammenfassend lässt sich sagen, dass die Paketquelle eines Logs (Netzwerk, Simulation oder Datei) unabhängig vom *Ziel* des Logs (Paketpuffer, Packet-Recording-Datei) eingestellt werden kann. Beachten Sie weiters, dass in jedem Fall alle Pakete, die nach Beenden eines Logs im Paketpuffer abgelegt sind, in eine Logdatei gespeichert werden können.

Um große Packet-Recording-Dateien in kleinere Teile aufzusplitten, und diese dann z.B. vollständig, ohne Paketverlust, zu loggen und als Logdateien zu speichern, wurde die 'Split PRC Files'-Funktion eingeführt. Sie wird über [Menü File | Split PRC Files...] aufgerufen. Die Größe der zu erzeugenden Dateien kann in den LPA-Einstellungen (siehe Abschnitt 5.11) konfiguriert werden. Die Dateinamen setzen sich aus dem Namen der Originaldatei sowie einer fortlaufenden Nummer zusammen. Die Datei 'test.prc' würde z.B. in die kleineren Dateien 'test0000.prc', 'test0001.prc', usw. aufgesplittet werden. Bitte haben Sie etwas Geduld, wenn Sie besonders große PRC-Dateien aufsplitten. Sobald alle Teildateien erzeugt wurden, erscheint eine Meldung über die Anzahl der resultierenden Dateien. Bitte beachten Sie, dass die Originaldatei bei diesem Vorgang immer erhalten bleibt.

5.11 LPA-Einstellungen

Generelle Einstellungen der LPA-Software können über [Menü File | Settings...] verändert werden. Durch Klick auf 'Default' können Sie jederzeit die letzten Standardeinstellungen wiederherstellen. Wenn Sie auf 'Save as Default' klicken, werden die aktuellen Einstellungen in der gespeichert und stellen somit die neuen Standardeinstellungen dar. Die Einstellungen werden außerdem automatisch gespeichert, wenn die LPA-Software beendet wird. Abbildung 48 zeigt den Einstellungsdialog.

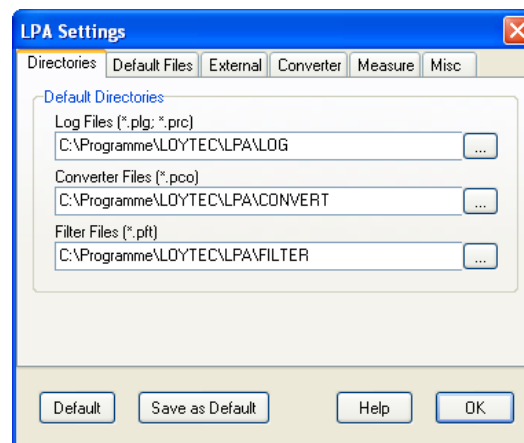


Abbildung 48: LPA-Einstellungen

Im oberen Bereich des Einstellungsdialogs sind die folgenden Gruppen auswählbar:

Directories

Hier können Sie Standardpfade für Logdateien (sowohl Standardlogdateien als auch Packet-Recording-Dateien), Konverterdateien und Filterdateien einstellen.

Default Files

Hier können Sie Dateien zur Voreinstellung der Paketfilter (Trigger, Aufzeichnungsfilter & Anzeigefilter) und des Paketkonverters angeben. Diese Dateien werden standardmäßig beim Start der LPA-Software für neue Paketlogs verwendet. Wenn Sie keine Voreinstellungen aus einer Datei wünschen, klicken Sie auf den 'Clear'-Knopf neben dem entsprechenden Eintrag.

External

Hier können Sie den LPA-Server aktivieren sowie ein LPA-Plug-In wählen. Der LPA-Server leitet alle empfangenen Pakete, welche das Aufzeichnungsfilter passieren, zu externen Applikationen (LPA-Clients) weiter. Bei einem LPA-Plug-In handelt es sich um eine externe DLL (Dynamic Link Library), welche die Übersetzungsfunktion und damit die Paketanzeige des LPA verändern kann. Weitere Informationen über die Entwicklung von LPA-Clients und -Plug-Ins finden Sie in Kapitel 6. Bitte beachten Sie, dass die Verwendung des LPA-Servers sowie von LPA-Plug-Ins die Aufzeichnungsgeschwindigkeit des LPAs herabsetzen kann.

Converter

Hier können Sie einige Einstellungen des Paketkonverters vornehmen. Wenn Sie 'Prompt before deleting Domains, Subnets or Groups' aktivieren, so erscheint bei jedem Löschversuch von Domains, Subnets oder Gruppen, deren Namen bereits in anderen Konverter- oder Filtertabellen verwendet werden, eine Sicherheitsabfrage. Dasselbe gilt in Bezug auf das Löschen von Knoten für 'Prompt before deleting nodes'. 'Prompt before changing corresponding Entries' bedeutet, dass bei jeder Änderung des Namens einer Domain, eines Subnets, einer Gruppe, eines Knotens oder einer Netzwerkvariable, welcher bereits anderswo in Verwendung ist, eine Abfrage erscheint, ob die entsprechenden Namenseinträge ebenfalls geändert werden sollen. Wird diese Einstellung nicht aktiviert, so werden Änderungen immer automatisch überall mitgezogen. Wird die Option 'Backup Converter Settings' deaktiviert, so beschleunigt dies signifikant die Verarbeitung großer Paketkonverterdateien. Manuelle Änderungen im Konverterdialog können dann allerdings nicht mehr rückgängig gemacht werden (per Cancel). Diese Option wurde eingeführt, um die Verwendung sehr großer Konverterdateien zu ermöglichen, welche z.B. mittels des LPAConv-Tools aus einer LNS-Datenbank generiert wurden.

Measure

Im 'Measurement System'-Feld können Sie zwischen SI-System und Imperialem US-System für die Anzeige von SNVTs auswählen. Im US-System existieren außerdem zusätzliche Anzeigoptionen. Beachten Sie, dass diese Optionen nur für SNVTs gelten, bei denen mehrere Anzeigeformate definiert sind.

Misc

Im „Time Stamp Settings“-Feld können Sie einstellen, ob die Hardware-Paketzeitstempel Ihres Netzwerk-Interfaces mit der Systemzeit Ihres PCs synchronisiert werden sollen. Dies kann nützlich sein, wenn andere Applikationen, die ebenfalls die Systemzeit anzeigen, parallel zum LPA laufen und ein Gleichlauf der Zeiten erwünscht ist. Beachten Sie jedoch, dass sich die relative Genauigkeit der Zeitstempel dadurch auf ca. 10µs verringert (statt 1µs). Im 'Packet Recording Files'-Feld können Sie die Größe der zu erzeugenden Dateien

beim Aufsplitten von Packet-Recording-Dateien einstellen. Die Größe ist in Mbytes (bis zu 64 MB) anzugeben. Im 'Export Settings'-Feld können Sie die Trennzeichen für exportierte CSV-Dateien (Comma Separated Value) einstellen. Standardmäßig werden die Trennzeichen den lokalen Windows-Einstellungen entnommen.

6 Externe Applikationen

In diesem Kapitel wird beschrieben, wie die LPA-Software in Verbindung mit anderen Applikationen eingesetzt werden kann. Es wird gezeigt, wie auf die Daten von Packet-Recording-Dateien zugegriffen werden kann, wie Pakete zu anderen Applikationen weitergeleitet werden können, sowie die Paketanzeige im LPA modifiziert werden kann. Entsprechende Beispielprogramme (in C) können Sie im Unterverzeichnis 'SOURCE' Ihres LPA-Installationsverzeichnisses finden.

6.1 Datenverarbeitung von Packet-Recording-Dateien

Da Packet-Recording-Dateien (siehe Abschnitt 5.10) ein sehr simples Format besitzen, ist es verhältnismäßig einfach, auf die enthaltenen Daten zuzugreifen. Im wesentlichen müssen dazu die entsprechende Datei geöffnet, der Dateikopf übersprungen und schließlich die Paketdaten kontinuierlich ausgelesen werden, bis das Ende der Datei erreicht ist. Jedes Paket besteht aus einer Längeninformation (2 Bytes), den eigentlichen Paketdaten (vom Priority-Bit bis zum CRC) und einem Zeitstempel. Die genaue Prozedur wird im Beispiel 'ProcPRC', welches im Unterverzeichnis 'SOURCE\ProcPRC' Ihres LPA-Installationsverzeichnisses zu finden ist, gezeigt. Die Datei 'ProcPRC.c' enthält den gesamten relevanten Quellcode des Beispiels. Die Projektdatei 'ProcPRC.sln' kann benutzt werden, um ein entsprechendes Projekt in Visual Studio 2010 zu öffnen. Die bereits übersetzte, ausführbare Datei 'ProcPRC.exe' ist im Unterverzeichnis 'SOURCE\ProcPRC\Release' zu finden. Bei Ausführung der Datei wird das Packet-Recording-File 'test.prc' gelesen, und die enthaltenen Paketdaten werden in einem Konsolenfenster angezeigt.

6.2 LPA-Server und -Clients

Der LPA kann während eines Logvorgangs Paketinformationen zu externen Applikationen weiterleiten. Diese Funktion wird durch Start des LPA-Servers aktiviert (siehe Abschnitt 5.11). Der LPA-Server schreibt alle Pakete, die das Aufzeichnungsfilter passieren, in einen Ringpuffer, welcher bis zu 128 Pakete aufnimmt. Sogenannte LPA-Clients können auf diese Daten online mittels der DLL 'LpaCli.dll' zugreifen. Diese DLL stellt zwei Funktionen zum Lesen von Paketen sowie Warten auf neue Pakete zur Verfügung. Um eine Blockierung der LPA-Software zu verhindern, existiert kein Hand-Shaking zwischen dem Server und den Clients. Dies bedeutet, dass alle Clients die Paketdaten schnell genug verarbeiten müssen, um keine Pakete zu verlieren. Ansonsten gibt es keinerlei Limitierung bezüglich der Zahl von gleichzeitig laufenden Clients. Weiters ist es möglich, sowohl die LPA-Clients als auch den LPA-Server jederzeit zu starten und zu beenden; die dazu notwendige Synchronisation wird immer automatisch vorgenommen. Um eine LPA-Client-Applikation zu entwickeln, muss die DLL (Dynamic Link Library) 'LpaCli.dll', welche sich im Unterverzeichnis 'SOURCE\LpaCliT\Release' Ihres LPA-Installationsverzeichnisses befindet, zu der Applikation gelinkt werden. Das Beispiel 'LpaCliT' im Unterverzeichnis

‘SOURCE\LpaCliT’ zeigt, wie die DLL zu verwenden ist. Es handelt sich dabei um eine einfache Applikation, welche alle Pakete vom LPA-Server liest und in einer Konsole ausgibt. Die Datei ‘LpaCliT.c’ enthält den Quellcode des Beispiels. In der Datei ‘LpaCli.h’ sind die beiden Funktion der DLL deklariert:

```
DWORD LpaCliWaitForPacket(    //wait for packet from LPA server
    DWORD Timeout            //timeout in ms (or INFINITE to wait infinitely)
);
```

Die LpaCliWaitForPacket-Funktion blockiert den aufrufenden Prozess (LPA-Client) solange, bis ein neues Paket vom LPA-Server empfangen wird, oder der Timeout-Wert überschritten wird. Um die Zeitbeschränkung auszuschalten, muss Timeout auf INFINITE (unendlich) gesetzt werden. Die Funktion liefert LPACLI_OK zurück, wenn ein neues Paket empfangen wurde und LPACLI_TIMEOUT wenn die zulässige Zeit (Timeout) überschritten wurde. Wenn ein fataler Fehler aufgetreten ist, liefert die Funktion LPACLI_COULD_NOT_START zurück.

```
DWORD LpaCliReadPacket(      //get next packet from LPA server
    LpaPacket_t *LpaPacket   //buffer that receives packet from LPA server
);
```

Die LpaCliReadPacket-Funktion liest das nächste Paket aus dem Ringpuffer des LPA-Servers. Der Parameter LpaPacket muss auf eine Struktur des Typs LpaPacket_t, welcher in ‘LpaPFmt.h’ deklariert ist, zeigen. Kann ein Paket gelesen werden, so werden die Paketdaten in diese Struktur geschrieben und die LpaCliReadPacket-Funktion liefert LPACLI_OK zurück. Falls kein Paket im Ringpuffer steht, liefert die Funktion LPACLI_NO_PACKET zurück. Im Falle eines fatalen Fehlers wird LPACLI_COULD_NOT_START zurückgeliefert. Aus der Datei ‘LpaPFmt.h’ (welche in ‘LpaCli.h’ inkludiert wird) wird lediglich die Deklaration der LpaPacket_t-Struktur für LPA-Clients benötigt. Alle anderen Deklarationen werden für LPA-Plug-Ins benötigt (siehe Abschnitt 6.3). Der Typ der LpaPacket_t-Struktur ist folgendermaßen deklariert (aus ‘LpaPFmt.h’):

```
typedef struct _LpaPacket_t    //LPA packet information
{
    //textual packet information
    char AbsoluteTime[32];      //absolute time stamp
    char ColLength[10];         //column 'Length'        in LPA packet table
    char ColFlags[16];          //column 'Flags'         in LPA packet table
    char ColTXNo[8];            //column 'TX#'           in LPA packet table
    char ColDomain[33];         //column 'Domain'        in LPA packet table
    char ColSource[128];        //column 'Source'        in LPA packet table
    char ColDestination[128];   //column 'Destination'   in LPA packet table
    char ColService[16];        //column 'Service'       in LPA packet table
    char ColData[1024];         //column 'Data'          in LPA packet table

    //numeric packet data
    BYTE RawPacket[8192];       //raw packet from priority bit to CRC
    DWORD Length;               //length of packet from first byte to CRC
    DWORD MessageStart;         //start of APDU (0 if no APDU)

    //additional packet information
    DWORD PacketId;             //packet ID
    DWORD PreambleLength;       //number of preamble bits before packet
    LONG TimeStampSec;           //seconds of packet timestamp
    LONG TimeStampNanoSec;      //nano seconds of packet timestamp
    DWORD Error;                 //greater than 0 if packet has errors
}LpaPacket_t;
```

Die textuelle Information setzt sich im wesentlichen aus den Spalten der entsprechenden Zeile der LPA-Pakettabelle zusammen (siehe Abschnitt 4.3). Ausnahmen bilden die Spalten ‘Number’ (welche nicht enthalten ist) und der Wert von AbsoluteTime, welcher immer dem kompletten, absoluten Zeitstempel entspricht, unabhängig von den LPA-Anzeigeoptionen (siehe Abschnitt 5.4). Die numerischen Informationen beinhalten das Paket in Rohform (RawPacket), die Länge des Pakets in Bytes (Length) und den Index des ersten Bytes der APDU (MessageStart). Wenn MessageStart=0 ist, so enthält das Paket keine APDU (z.B. bei Acknowledgements). Zusätzlich wird noch die Preamblelänge des Pakets (PreambleLength), der Zeitstempel in numerischer Form (TimeStampSec, TimeStampNanoSec), das Fehlerflag (Error), und eine Paket-ID (PacketId) zurückgeliefert. Der Wert von TimeStampSec kann in einen Datumswert und einen Zeitwert aufgesplittet werden, wie im Beispiel ‘ProcPRC’ (‘SOURCE\ProcPRC\ProcPRC.c’) demonstriert wird. Die Paket-ID beginnt bei 0 wenn der LPA-Server gestartet wird und erhöht sich wann immer ein neues Paket vom Server

geschrieben wird. Sie kann im Client benutzt werden, um verloren gegangene Pakete zu detektieren.

Das Beispiel 'LpaCliT' enthält eine Visual Studio 2010 Projektdatei namens 'LpaCliT.sln'. Folgende Einstellungen wurden dabei in Visual Studio vorgenommen: Im [Menü Project | Configuration Properties | C/C++ | Code Generation] ist das 'Struct Member Alignment' auf 1 Byte gesetzt. Dies ist für eine korrekte Zusammenarbeit mit der LPA-Client-DLL unerlässlich. Im [Menü Project | Properties | Linker | Input] wurde 'LpaCli.lib' zu den 'Additional Dependencies' hinzugefügt. Die entsprechende Library-Datei 'LpaCli.lib' befindet sich im Unterverzeichnis 'SOURCE\LpaCliT' Ihres LPA-Installationsverzeichnisses. Die bereits übersetzte, ausführbare Datei 'LpaCliT.exe' ist im Unterverzeichnis 'SOURCE\LpaCliT\Release' zu finden. Wenn dieser LPA-Client bei aktiviertem LPA-Server ausgeführt wird, können alle geloggte Pakete im Konsolenfenster des Clients beobachtet werden. Beachten Sie, dass der Client, wie oben beschrieben, auch mehrmals gestartet werden kann.

6.3 LPA-Plug-Ins

Die Anzeige der Paketinformation im LPA kann mittels eines LPA-Plug-Ins und dessen Aktivierung in den LPA-Einstellungen (siehe Abschnitt 5.11) modifiziert werden. Dies kann verwendet werden, um anwendungsspezifische Daten (benutzerdefinierte Netzwerkvariablen, Explicit.-Messages, Foreign-Frames, etc.) in interpretierter Form darzustellen. Ein LPA-Plug-In ist eine DLL (Dynamic Link Library), welche vom LPA benutzt wird, wann immer Paketdaten angezeigt werden sollen. In der DLL müssen folgende zwei Funktionen implementiert sein:

```
BOOL LpaPlgChangePacket(           //change packet display in LPA packet table
    LpaDisplayOptions_t *LpaDisplayOptions, //current LPA display options
    LpaPacket_t *LpaPacket          //packet to be displayed in packet table
)
```

Die LpaPlgChangePacket-Funktion wird vom LPA kurz vor Anzeige jedes Pakets in der Pakettabelle aufgerufen. Die Paketinformation wird mittels des Parameters LpaPacket übergeben. Dieser hat dasselbe Format wie bei den LPA-Clients (siehe Abschnitt 6.2). Die textuelle Information der Struktur entspricht dabei jener, welche in der Pakettabelle angezeigt werden soll. In der LpaPlgChangePacket-Funktion muss nun entschieden werden, ob diese Information vor der Ausgabe verändert werden soll. Dies betrifft die Werte ColDomain, ColSource, ColDestination und ColData (und somit die Spalten 'Domain', 'Source', 'Destination' und 'Data'), welche einfach in der LpaPlgChangePacket-Funktion überschrieben werden können. Falls eine derartige Wertänderung vorgenommen wurde, muss die Funktion TRUE zurückliefern, ansonsten FALSE. Im Parameter LpaDisplayOptions werden die aktuellen Werte der LPA-Anzeigeoptionen (siehe Abschnitt 5.4) übergeben. Diese können z.B. zur Formatierung (dezimal oder hexadezimal) von Integer-Werten gemäß den eingestellten Optionen verwendet werden.

```
BOOL LpaPlgChangePacketDetails( //change display of LPA packet details
    LpaDisplayOptions_t *LpaDisplayOptions, //current LPA display options
    LpaPacket_t *LpaPacket, //packet to be displayed in detail
    LpaPacketDetails_t *LpaPacketDetails //buffer that receives packet details
)
```

Die LpaPlgChangePacketDetails-Funktion wird vom LPA kurz vor Anzeige eines Pakets in den Paketdetails des Logfensters aufgerufen (siehe Abschnitt 4.3). Wie bei der vorangegangenen Funktion, wird auch hier die LpaPacket-Struktur übergeben, um eine Entscheidung bezüglich Modifikation der Ausgabe zu ermöglichen. Der Parameter LpaDisplayOptions hat ebenfalls dieselbe Bedeutung wie bei der LpaPlgChangePacket-Funktion. Zusätzlich wird noch der Parameter LpaPacketDetails übergeben, welcher die textuellen Informationen enthält, die in den Paketdetails angezeigt werden sollen. Die entsprechende Struktur hat folgendes Format (aus 'LpaPFmt.h'):

```
typedef struct _LpaPacketDetails_t //LPA packet details (for LPA plugins)
{
    char FieldDomain[33]; //field 'Domain' in LPA packet details
    char FieldSource[128]; //field 'Source' in LPA packet details
    char FieldDestination[128]; //field 'Destination' in LPA packet details
    char FieldMessage[64]; //field 'Message' in LPA packet details
    char **FieldData; //field at the bottom of LPA packet details
} LpaPacketDetails_t;
```

Die Werte von `FieldDomain`, `FieldSource`, `FieldDestination` und `FieldMessage` entsprechen den Feldern 'Domain', 'Source', 'Destination' und 'Message' der Paketdetails. `FieldData` ist ein Array von Strings, welches den Datenbereich am unteren Ende der Paketdetails repräsentiert. Die maximale Zeilenzahl in `FieldData` ist mit `LPA_PDET_MAX_LINES` beschränkt, die maximale Länge einer Zeile mit `LPA_PDET_MAX_CHARS`. Wenn nicht alle Zeilen benutzt werden, muss die Zeile nach der letzten benutzten Zeile auf den Null-String gesetzt werden (`FieldData[Lastline+1][0]='\0'`). Alle Strings der `LpaPacketDetails`-Struktur können in der `LpaPlgChangePacketDetails`-Funktion überschrieben werden. Falls eine derartige Änderung vorgenommen wurde, muss die Funktion `TRUE` zurückliefern, ansonsten `FALSE`. Beachten Sie, dass Plug-Ins im Kontext der LPA-Software laufen und daher - bei fehlerhafter Programmierung - diese auch zum Absturz bringen können.

Das Beispiel 'LpaPlgT' zeigt die korrekte Implementierung einer LPA-Plug-In-DLL. Es befindet sich im Unterverzeichnis 'SOURCE\LpaPlgT' Ihres LPA-Installationsverzeichnisses. Die Datei 'LpaPlgT.c' enthält den Quellcode der DLL. Die Datei 'LpaPfmt.h', welche alle nötigen Struktur- und Konstantendeklarationen enthält, ist in 'LpaPlgT.c' inkludiert. Die Datei 'LpaPlgT.def' wird zum Exportieren der beiden DLL-Funktionen verwendet. Auch bei diesem Beispiel ist eine Visual Studio 2010 Projektdatei namens 'LpaPlgT.sln' enthalten. Folgende Einstellungen wurden in Visual Studio vorgenommen: Im [Menü Project | Configuration Properties | C/C++ | Code Generation] wurde das 'Struct member alignment' auf 1 Byte sowie die 'Runtime Library' auf 'Multithreaded DLL' gesetzt. Im [Menü Project | Configuration Properties | C/C++ | Advanced] wurde die 'Calling Convention' auf '`__cdecl`' gesetzt.

Alle drei Einstellungen sind für die korrekte Zusammenarbeit mit der LPA-Plug-In-Schnittstelle unerlässlich. Eine bereits übersetzte Version der DLL 'LpaPlgT.dll' befindet sich in den Unterverzeichnissen 'SOURCE\LpaPlgT\Release' sowie 'PLUGIN'. Sie kann, wie in Abschnitt 5.11 beschrieben, im LPA aktiviert werden. Die Darstellung aller 'Application-Messages' mit Message-Code 5 wird daraufhin, wie in Abbildung 49 gezeigt, verändert.

The screenshot shows the 'Active Log Running' window with a table of network traffic. The selected packet (Number 1) is detailed in the 'General Packet Information' and 'Address and Message Information' sections. The 'Data' field shows the hex sequence: 0000: 00 00 01 81 01 00 05 FF 94 51.

Number	Time	Length	Flags	TX#	Domain	Source	Destination	Service	Data
1	14:50:29.597000	10	-- -- --	0	PLUGIN Domain	PLUGIN Source	PLUGIN Destination	ACKD	PLUGIN Data
2	14:50:54.644000	10	-- -- --	0	PLUGIN Domain	PLUGIN Source	PLUGIN Destination	ACKD	PLUGIN Data
3	14:50:54.800000	10	-- -- --	0	PLUGIN Domain	PLUGIN Source	PLUGIN Destination	ACKD	PLUGIN Data

General Packet Information

Packet Number: 1
 Time: 2006/01/13 14:50:29.597000
 Length: 10 DataLength: 1
 TX Number: 0 CRC: 5194
 Service: Acknowledged

Address and Message Information

Domain: PLUGIN Domain
 Source: PLUGIN Source
 Destination: PLUGIN Destination
 Message: PLUGIN Message Type

PLUGINS Data Line 0x01
 PLUGINS Data Line 0x02
 PLUGINS Data Line 0x03

PREAMBLE LENGTH: 16
 PPDU HEADER (LINK/MAC PROTOCOL DATA UNIT)
 NPDU HEADER (NETWORK PROTOCOL DATA UNIT)
 TPDU HEADER (TRANSPORT PROTOCOL DATA UNIT)
 APDU (APPLICATION PROTOCOL DATA UNIT)
 Application Message or Response 05 (005)
 Data0000: FF -- -- -- -- -- | .
 CRC 5194

0000: 00 00 01 81 01 00 05 FF 94 51

Abbildung 49: LPA-Plug-In

6.4 LPA Report-DLLs

Für die Erstellung einer kundenspezifischen Report-Vorlage (siehe Abschnitt 5.7) wird die LPA Report-DLL Schnittstelle verwendet. Dabei muss die Funktion `LparGenerateReport` in der DLL implementiert werden:

```
DWORD LparGenerateReport (
    LparGetUint_t *LparGetUint, //function to get an unsigned integer value
    LparGetStr_t *LparGetStr,   //function to get a character array
    LparAddLine_t *LparAddLine //function to add a new line to report
)
```

Die Funktion wird vom LPA immer dann aufgerufen, wenn der Benutzer einen Report anfordert. Bei den drei Parametern handelt es sich um Callback-Funktionen, welche die DLL zur Protokollerstellung verwenden muss. Die Funktionsprototypen sind in 'SOURCE\LpaRpt\LpaRpt.h' definiert:

```
typedef DWORD __cdecl LparGetUint_t(
    DWORD Type, //type of statistics value (general, etc.)
    DWORD ItemIdx, //item index if not general type
    DWORD ValueIdx //value index
);
```

Die Funktion `LparGetUint` wird verwendet, um einen bestimmten Integer-Wert von der LPA-Statistik des aktuellen Logs abzurufen. Der Parameter `Type` spezifiziert den Typ des gewünschten Werts: `LPAR_GEN` spezifiziert allgemeine Statistikwerte, wie die absolute Paketanzahl oder die Anzahl von fehlerhaften Paketen. `LPAR_DOM`, `LPAR_SUB`, `LPAR_NOD`, `LPAR_GRP` spezifizieren Werte, welche mit einer bestimmten Domain, einem Subnet, einem Knoten oder einer Gruppe assoziiert sind. In diesem Fall wird im Parameter `ItemIdx` der Index der Domain, des Subnets, des Knotens oder der Gruppe festgelegt. Ansonsten (`Type=LPAR_GEN`) muss `ItemIdx` auf 0 gesetzt werden. `ValueIdx` spezifiziert schließlich den Index des gewünschten Werts. Die verfügbaren Wert-Indices sind in 'SOURCE\LpaRpt\LpaRpt.h' definiert und dokumentiert.

```
typedef const char* __cdecl LparGetStr_t(
    DWORD Type, //type of statistics value (general, etc.)
    DWORD ItemIdx, //item index if not general type
    DWORD ValueIdx //value index
);
```

Die Funktion `LparGetStr` wird verwendet, um einen bestimmten String von der LPA-Statistik des aktuellen Logs abzurufen. Der Parameter `Type` spezifiziert den Typ des gewünschten Strings: `LPAR_GEN` spezifiziert allgemeine Strings, wie den LPA Versionsstring oder den Logdateinamen. `LPAR_DOM`, `LPAR_SUB`, `LPAR_NOD`, `LPAR_GRP` spezifizieren Strings, welche mit einer bestimmten Domain, einem Subnet, einem Knoten oder einer Gruppe assoziiert sind. In diesem Fall wird im Parameter `ItemIdx` der Index der Domain, des Subnets, des Knotens oder der Gruppe festgelegt. Ansonsten (`Type=LPAR_GEN`) muss `ItemIdx` auf 0 gesetzt werden. `ValueIdx` spezifiziert schließlich den Index des gewünschten Strings. Die verfügbaren String-Indices sind in 'SOURCE\LpaRpt\LpaRpt.h' definiert und dokumentiert.

```
typedef void __cdecl LparAddLine_t(
    LONG Mode, //line add mode (must be set to LPAR_MNORM)
    void *Line, //line to add (must point to character array)
    LONG InsNo //line number to insert (LPAR_END to append)
);
```

Die Funktion `LparAddLine` wird verwendet, um dem Report eine neue Zeile hinzuzufügen. Der Parameter `Mode` muss auf `LPAR_MNORM` gesetzt werden. Der Parameter `Line` muss auf den String (ein Character-Array) zeigen, welcher die neue Zeile beinhaltet. Der Parameter `InsNo` spezifiziert die Zeilennummer, in die die neue Zeile eingefügt werden soll. Um die Zeile am Ende anzuhängen, muss `InsNo` auf `LPAR_END` gesetzt werden.

Das Verzeichnis 'SOURCE\LpaRpt' in Ihrem LPA-Installationsverzeichnis enthält den kompletten Source-Code der englischen und deutschen LOYTEC Report-DLLs. Beide Projekte sind in der Visual Studio 2010 Solution-Datei 'LpaRpt.sln' integriert. Eine Übersetzung dieser Vorlage in eine andere Sprache kann einfach durch Übersetzung der Dateien 'LpaRptLocEng.h' oder 'LpaRptLocGer.h' erfolgen. Strukturelle Änderungen der

Vorlage sind in 'LpaRpt.c' möglich. Die fertige DLL muss schließlich entsprechend umbenannt und in das 'RPTTYPE'-Verzeichnis kopiert werden. Beim nächsten Start des LPAs wird die DLL dann automatisch den bestehenden Vorlagen hinzugefügt.

7 Versionsverzeichnis

Datum	Version	Autor	Beschreibung
11.05.2000	2.3	AB	Erste Version
22.01.2001	2.4	AB	Neue Funktionen des LPA v2.4
11.12.2001	2.5	AB	Neue Funktionen des LPA v2.5
23.07.2002	2.6	AB	Neue Funktionen des LPA v2.6
02.06.2003	2.7	AB	Neuer Abschnitt 2.3 Netzwerk-Interface- und Transceiver, LPA-IP Funktionen (LPA auf NIC852, siehe 2.3.2 and 2.3.3), "Multiplexed Network Interfaces" (MNI-Geräte, siehe 2.3.4), Kleine Änderungen und Anpassungen in allen anderen Kapiteln.
29.01.2004	2.8	AB	Zahlreiche Änderungen in Kapitel 2 Installation und Konfiguration, Neuer Abschnitt 2.3.4 NIC-IP Geräte.
23.02.2004	2.9	AB	Einige kleinere Änderungen
24.01.2005	2.11	AB	Zusätzliche Informationen im Netzwerk-Interface Dialog, siehe Abbildung 2 und Abbildung 14, Verbesserte Dokumentation des Packet Storage Modes in Abschnitt 5.1, Kapitel 6: Alle Beispielprojekte auf Visual C++ 7.1 umgestellt.
25.02.2005	2.12	AB	LPA Server-Modus, siehe Abschnitt 2.7, erweitertes Filtern auf APDU-Basis, siehe Abschnitt 5.3.
04.04.2005	2.13	AB	Einige kleinere Änderungen
18.01.2006	3.0	AB	Neuer Abschnitt 2.4 Datei Öffnen mittels Kommandozeile, Abschnitt 4.3: Transaktionsidentifikation hinzugefügt, Abschnitt 4.6: 'Adjust Columns' und Filter / Konvertierung, Abschnitt 4.8: LPA 3.0 Informationen in Logdateien hinzugefügt, Abschnitt 5.1: Neues Feld 'Trend Size', Abschnitt 5.5: Neue Fehlerzähler, Neuer Abschnitt 5.6 Knotenstatistik, Neuer Abschnitt 5.7 LPA-Reports, Neuer Abschnitt 5.8 Statistiktrend, Neuer Abschnitt 6.4 LPA Report-DLLs.
07.03.2007	3.1	AB	Einige kleine Änderungen und Korrekturen.
13.07.2007	3.2	AB	Bis zu 512 L-IPs können nun zugewiesen werden, Abschnitt 2.3.3, Bis zu 512 NIC-Ips können nun zugewiesen werden, Abschnitt 2.3.4.
14.01.2008	3.3	AB	Verwendung des Standardterms „CEA“ statt „EIA“. Allgemeine Remote-LPA Unterstützung (nicht auf L-Ips beschränkt), siehe Abschnitt 2.3.3. NIC-IP Konfiguration entfernt, siehe Abschnitt 2.3.4.

Datum	Version	Autor	Beschreibung
11.08.2008	3.4	AB	Unterstützung des software-aktivierten NIC852-SW, siehe Abschnitt 2.3.2.
02.02.2010	3.5	AB	Unterstützung von 64-Bit Windows Betriebssystemen.
06.08.2010	3.6	AB	Unterstützung neuer Remote LOYTEC Geräte.
02.05.2013	3.7	AB	Unterstützung von Windows 8/2012 (64 Bit). Kapitel 6: Alle Beispielprojekte auf Visual Studio 2010 umgestellt. Abschnitt 2.2: LPA Registrierung erfolgt nun in der LPA Software. DNS Fähigkeit hinzugefügt in Abschnitt 2.3.3.

Abkürzungen

ACK	...	Acknowledgement
ACKD	...	Acknowledged Message
APDU	...	Application Protocol Data Unit
AuthPDU	...	Authentication Protocol Data Unit
CNIP	...	Control Network over IP
CRC	...	Cyclic Redundancy Check
CSV	...	Comma Separated Values
DLL	...	Dynamic Link Library
LAN	...	Local Area Network
LPA	...	LOYTEC Protokollanalysator
Mbps	...	Megabits pro Sekunde
MDI	...	Multiple Document Interface
MNI	...	Multiplexed Network Interface
NID	...	Unique Node ID
NPDU	...	Network Protocol Data Unit
NV	...	Netzwerkvariable
PDU	...	Protocol Data Unit
SNVT	...	Standardnetzwerkvariablentyp
SPDU	...	Session Protocol Data Unit
TPDU	...	Transport Protocol Data Unit
WAN	...	Wide Area Network

Abbildungsverzeichnis

Abbildung 1: LPA Software-Registrierung	6
Abbildung 2: Netzwerk-Interface Auswahl	7
Abbildung 3: NIC709-Aufbau	8
Abbildung 4: NIC709 Transceiver-Auswahl	8
Abbildung 5: LPA-IP auf NIC852	9
Abbildung 6: Paketaufzeichnung auf CEA852	9
Abbildung 7: NIC852 Transceiver-Auswahl	10
Abbildung 8: Remote-LPA auf L-IP	11
Abbildung 9: Remote LPA Assignment	11
Abbildung 10: Zuweisen/Hinzufügen eines Remote-LPA Geräts	12
Abbildung 11: Hinzufügen eines CEA852-Kanals	12
Abbildung 12: Transceiver-Anzeige für Remote-LPA Geräte	13
Abbildung 13: Multiplexed Network Interfaces	14
Abbildung 14: Expert Mode bei der Netzwerk-Interface-Auswahl	14
Abbildung 15: LPA-Server Systray-Icon	16
Abbildung 16: Systray-Icon Menü	16
Abbildung 17: Aktives Logfenster	17
Abbildung 18: Eintreffende Pakete	17
Abbildung 19: Paketdetails	18
Abbildung 20: Konvertierte Pakete	18
Abbildung 21: Paketstatistikfenster	19
Abbildung 22: Ende der Demonstrationsdatei	20
Abbildung 23: Logfenster einer Paketlogdatei	20
Abbildung 24: LPA-Hauptfenster	21
Abbildung 25: Knopf mit zugehörigem Menüpunkt	22
Abbildung 26: Logfenster	24
Abbildung 27: Netzwerkmanagement- und -diagnosenachrichten	25

Abbildung 28: SNVT-Nachrichten	26
Abbildung 29: Statusleiste	26
Abbildung 30: Suchen von Paketen	27
Abbildung 31: Anspringen von Paketen	28
Abbildung 32: Kontextmenü (View-Menü)	28
Abbildung 33: Print Log	31
Abbildung 34: Logmodus	32
Abbildung 35: Paketkonverter	34
Abbildung 36: Knoteneditor	35
Abbildung 37: Paketfilter	37
Abbildung 38: Adress- und APDU-Tabelle	38
Abbildung 39: Adresseditor	38
Abbildung 40: Anzeigeoptionen	41
Abbildung 41: Paketstatistik für normales Logfenster und Aktiven Log	42
Abbildung 42: Knotenstatistik	44
Abbildung 43: Kontextmenü der Knotenstatistik	47
Abbildung 44: LPA-Report	47
Abbildung 45: Statistiktrend	49
Abbildung 46: Paketsimulation	50
Abbildung 47: Paketerzeugung	50
Abbildung 48: LPA-Einstellungen	52
Abbildung 49: LPA-Plug-In	58

Index

A

Absenderadresse.....	27, 41
Acknowledged.....	47
Adress- und APDU-Tabelle	39
Adresseditor	40
Adressformat	43
Aktiver Log	23
Aktualisierung anhalten.....	25
Alternate-Path	47
Anzeigefilter.....	25, 38, 48
Anzeigeoptionen	25, 43
APDU.....	28, 39, 53
APDU-Eintrag.....	42
Applikationsnachrichten.....	27
ASCII.....	27
Aufzeichnungsfilter	25, 38
Ausgangsnetzwerkvariable.....	37
ausgeblendete Pakete	31, 45
AuthPDU.....	28
AuthPDU-Header.....	53

B

Bandbreitenausnutzung	45
Broadcast	27

C

CEA709.....	6
CEA852.....	6
CEA852.....	11
corrupted packets	45

CRC 52

CRC-Fehler	29
CSV-Datei.....	32, 49, 51, 56

D

Dateivoreinstellungen	55
Daten.....	27
Datenformat	43
Datenmaske	42
Demonstrationsdatei.....	21
DLL 57, 59, 61	
Domain.....	27, 36, 41, 46

Domain-ID	36, 37, 41
Domainindex.....	38
Domaintabellen	37
Drucken.....	32

E

Eingangsnetzwerkvariable	37
Empfängeradresse	27, 41
erweiterte Funktionen.....	34
Exporeinstellungen	56
Exportieren.....	32, 49, 51
externe Applikationen	55, 57

F

fehlerhafte Pakete.....	44, 45
Fehlerzähler	45
Filterdatei	38
Filtersektion	39
Flags.....	26

G	
Gruppe	27, 36, 37, 38, 41, 46
Gruppen-ID	36
H	
Hauptfenster	23
Hilfedatei.....	33
I	
Installation.....	7
Interface Settings.....	8
Interface-Einstellungen	24
interrupted packets	45
IP-852.....	10
K	
Kanalteilnehmer	12
Knoten.....	36, 46
Knoteneditor	36
Knoteninformation	37
Knotenname	37, 41
Knotennummer.....	27, 37, 38, 41
Kommandozeilenparameter.....	16
Kontextmenü.....	30, 49
Konverterdatei.....	35
Konvertereinstellungen	55
Konverteroptionen	43
korrekte Pakete.....	44, 52
L	
Langzeitaufzeichnung	54
LConfig	7
L-IP	11
Log beenden.....	21, 25
M	
Log löschen.....	25
Log öffnen.....	24
Log speichern.....	24
Log unterbrechen	20, 25
Log vom Netzwerk.....	25, 31
Logdatei	23, 31
Logfenster	26
Logmodus	24, 34
Logstatus.....	28
LOYTEC Konfigurations-Tool.....	7
LOYTEC Protokollanalysator.....	6
LPA 6	
LPA beenden.....	22
LPA Menüs	23
LPA Software.....	7
LPA-Client.....	57
LPAConv	56
LPA-Einstellungen.....	54
LPA-IP	6, 9, 11
LPA-IP-SW	6
LPA-Konfigurationen	16
LPA-Plug-In.....	45, 55, 59
LPA-Server	45, 55, 57
LPA-Server-Modus.....	17
LPA-SW	6
M	
markierte Pakete.....	31, 45
MD5-Authentifizierung.....	13
MDI 23	
Menüpunkt	23

Meßsystem	56	Pakete ausblenden	31
Missed Preambles	45	Pakete markieren.....	31
MNI-Geräte.....	14	Pakete suchen.....	25, 29
Multiplexed Network Interfaces.....	14	Paketerzeugung	52
N			
Nachrichtentyp	45	Paketfilter.....	30, 38
negativer Eintrag	40	Paketkonverter	25, 30, 35, 49
Netzwerkadressen	35, 39	Paketlänge	26, 44
Netzwerkdiagnosenachrichten.....	27	Paketlog	23
Netzwerk-Interface.....	6, 8, 24	Paketpuffer.....	34
Netzwerk-Interface Konfiguration	7	Paketsimulation.....	51
Netzwerkmanagementnachrichten.....	27	Paket Speichermodus.....	34
Netzwerkvariablen	37, 42	Paketstatistik	26, 44
neuer Log	24	Pakettable	26
NIC709.....	7, 8	Pass Packets	41
NIC852.....	7, 9, 11	PC	6
NIC-IP.....	14	PDU-Format.....	45
NID	27, 37, 41	Personal Firewall	7
NodeNr.....	37	positiver Eintrag.....	40
NPDU.....	28	PPDU	28
NPDU-Header.....	53	PPDU-Header	52
O			
On-line-Modus	31, 35	PRC-Dateien aufsplitten.....	54
P			
Packet-Recording-Datei	34, 53, 56, 57	Protokoll details	28
Paketdetails	27	Protokoll details ausblenden	31
Paketdetails ausblenden	31	Protokoll details einblenden.....	31
Paketdetails einblenden.....	31	Protokollfehler	27, 45, 52
Paketdurchsatz	52	Q	
Pakete anspringen.....	25, 29, 51	Querformat.....	33
R			
		Receiver	47
		Registrierung.....	7

Reject Packets	41	Subnet	27, 36, 37, 38, 41, 46
Remote Device Assignment	11	Subnet-ID	36
Remote Device Discovery	11	symbolischer Name	35
Remote LPA	6		
Remote-LPA	11	T	
Report	49, 61	Tastenkombination	23, 31
Richtung	37, 42	TPDU	28
		TPDU-Header	53
S		Trace-Modus	53
Schicht 2	52	Transaktionsidentifikation	27
Schicht 3	53	Transaktionsnummer	26
Schicht 4	53	Transceiver	28
Schicht 5	53	Transceiver-Auswahl	8
Schriftartgröße	33	Trend	34, 50
Selektor	37, 42	Trigger	24, 39
Sender	47		
Service	27, 45	U	
SNVT	27, 38	USB-Key	9
Sortierung	47		
Spalten ausblenden	30	V	
Spalten einblenden	30	verlorene Pakete	29
Spaltenanpassung	30, 48		
SPDU	28	W	
SPDU-Header	53	Werkzeuggestreife	24
Standardpfade	55		
Starten eines Logs	19	Z	
Statusleiste	28	Zeilennummer	26, 29
Stummer Knoten	47	Zeitstempel	14, 16, 26, 54, 56
		Zeitstempelformat	43
		Zeitstempelmodus	43
		Zusammenfügen von Konverterdateien	35