1 Netzwerkanalyse White Paper

Dieser Anwendungshinweis gibt Tipps und Ratschläge zur Fehlersuche in EIA709 Netzwerken. Es beschreibt, wie LOYTEC's LPA Protocol Analyzer verwendet werden kann, um Netzwerkfehler schnell und effizient zu finden und zu beheben.

2 Vorgangsweise bei der Netzwerkanalyse

Basis einer erfolgreichen und effizienten Fehleranalyse ist ein definierter Arbeitsablauf. Abbildung 1 zeigt das Flussdiagramm der empfohlenen Vorgangsweise bei der Fehlersuche.

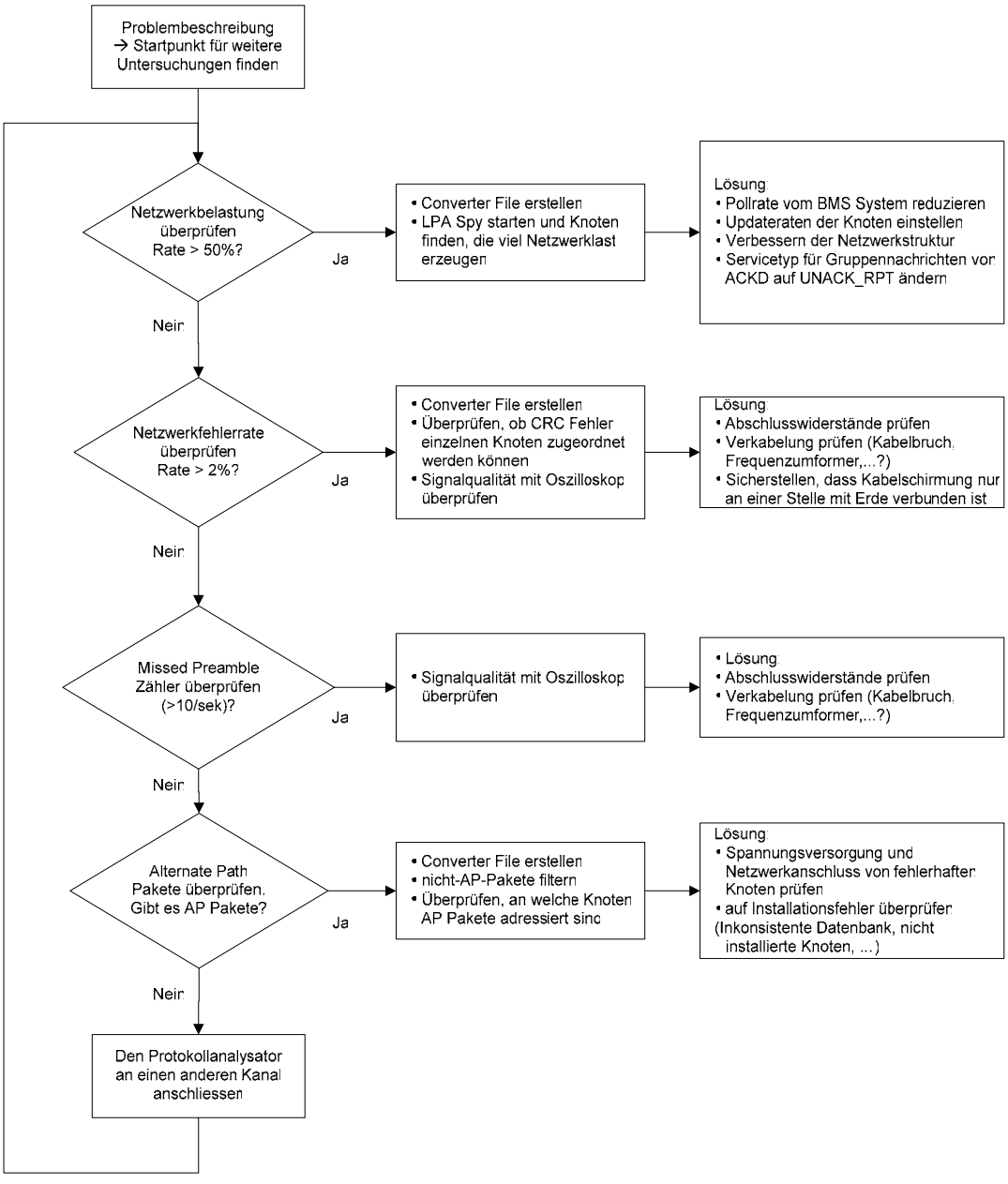

Abbildung 1: Arbeitsschritte für eine Fehleranalyse von EIA 709 Netzwerken.

2.1 Problembeschreibung

Am Beginn jeder Netzwerkanalyse ist es wichtig, sich eine Überblick über das Netzwerk und die bestehenden Probleme zu verschaffen. Anstatt den Protokollanalysator an des Netzwerk anzuschließen und wahllos Daten zu sammeln wird dringend empfohlen, das Problem mit den Ingenieuren vor Ort zu diskutieren und daraus wertvolle Hinweise für die Fehlersuche zu erhalten.

Dabei sind beispielsweise folgende Fragen zu erläutern:

1. ***Welches Problem ist** auf dem Netzwerk aufgetreten? Wie äußert sich das Problem?*

   Bestehen Kommunikationprobleme auf dem Netzwerk? Können manche Knoten auf dem Netzwerk nicht erreicht werden oder werden manche Knoten in der Visualisierung als „offline“ markiert?

2. ***Welche Teile des Netzwerks** sind betroffen?*

   Treten die Probleme am gesamten Netzwerk oder nur in einzelnen Netzwerksegmenten oder nur bei einzelnen Knoten auf?

3. ***Wann** tritt das Problem auf?*

   Besteht das Problem permanent oder tritt es nur unter bestimmten Umständen (z.B. zu bestimmten Zeiten oder in bestimmten Situationen) auf?

4. *Wie ist das **Netzwerk strukturiert**?*

   Gibt es einen Backbone-Kanal? Welche Kanaltypen werden verwendet? Wie viele Knoten sind an die einzelnen Netzwerksegmente angeschlossen? Wie lang sind die Netzwerksegmente? Zumeist ist es hilfreich, eine Skizze der Netzwerkstruktur zu erstellen und die fehlerhaften Bereiche darin zu markieren.

5. *Wie hoch ist die **Kommunikationsrate** auf dem Netzwerk?*

   Welche Knoten kommunizieren untereinander? Gibt es ein Visualisierungssystem, das Werte abfragt? Wie hoch ist die erwartete Netzwerkbelastung in den Segmenten?

6. *Wurden **Veränderungen** am Netzwerk vorgenommen?*

   Wurde das Netzwerk bereits einmal störungsfrei betrieben? Wurden Veränderungen am Netzwerk vorgenommen, bevor die Probleme aufgetreten sind?

Die gesammelten Informationen werden dazu verwendet, einen Ansatzpunkt für eine Fehlersuche mit dem LPA Protocol Analyzer zu finden. Die in den LOYTEC Netzwerk Infrastrukturprodukten (L-Switch, L-IP) eingebauten Diagnosefunktionen liefern ebenfalls Basisinformationen für die Netzwerkdiagnose. Rot blinkende Diagnose-LEDs auf diesen Geräten zeigen Fehler in den angeschlossenen Netzwerksegmenten an. Daher ist es nahe liegend, diese Segmente mit dem LPA Protocol Analyzer genauer zu untersuchen, um die Art des Fehlers und die Fehlerursachen näher zu erkunden.

3 Netzwerkanalyse

Die gesammelten Informationen müssen nun ausgewertet werden, um zu entscheiden, an welcher Stelle im Netzwerk der LPA Protokollanalysator zuerst eingesetzt werden soll. Wenn nur einzelne Knoten von den Netzwerkproblemen betroffen sind, so sollte der Analysator zunächst in der Nähe der betroffenen Knoten angeschlossen werden. Kommunikationsprobleme zwischen dem Visualisierungssystem und den Knoten können am Besten analysiert werden, indem man das Analysetool an den Kanal der Visualisierung anschließt. Auch der Backbone-Kanal des Systems ist oft ein guter Punkt, um mit der Netzwerkanalyse zu beginnen, falls die Problemanalyse keine genaueren Anhaltspunkte liefert.

3.1 Bandbreitenauslastung

Das Netzwerk Statistikfenster gibt einen Überblick über den Gesundheitszustand des Kanals. Das Fenster wird über die „Statistic“ Schaltfläche oder über den Menüeintrag „Statistics“ im „Packet“-Menü aufgerufen, während der Log-Vorgang läuft. Der erste zu überprüfende Parameter ist die Bandbreitenauslastung des Kanals (network bandwidth utilization) auf dem „General“ Karteireiter des Fensters (siehe Abbildung 2).

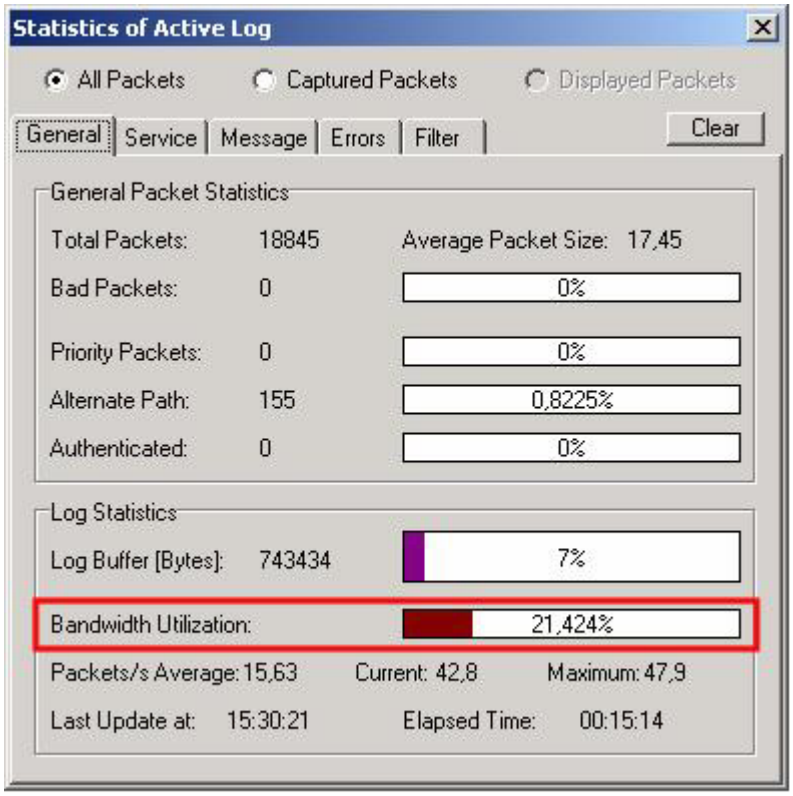

Abbildung 2: Kanalauslastung

Die Kanalauslastung sollte Werte von ungefähr 50% nicht übersteigen. Höhere Messwerte erfordern eine genauere Untersuchung, besonders der Knoten im Netzwerk welche zur Kanalauslastung beitragen. Um Knoten auf dem Netzwerk einfach zu identifizieren, kann mit Hilfe des LPAConv LNS Plugins ein LPA Converter Files aus einer LNS Datenbank erstellt

werden. Mit Hilfe der Konverterdatei übersetzt der LPA Netzwerkadressen (Subnet/Node Adresse, Node IDs, u.s.w.) in Knotennamen, wie sie im LNS Projekt vergeben wurden. Das LPASpy Programm verwendet ebenfalls diese Namen, um die Netzwerkdaten anzuzeigen (siehe Abbildung 3). Es wertet die gesammelten Daten aus, um anzuzeigen, wie viel der Netzwerkbandbreite von den einzelnen Knoten belegt wird.

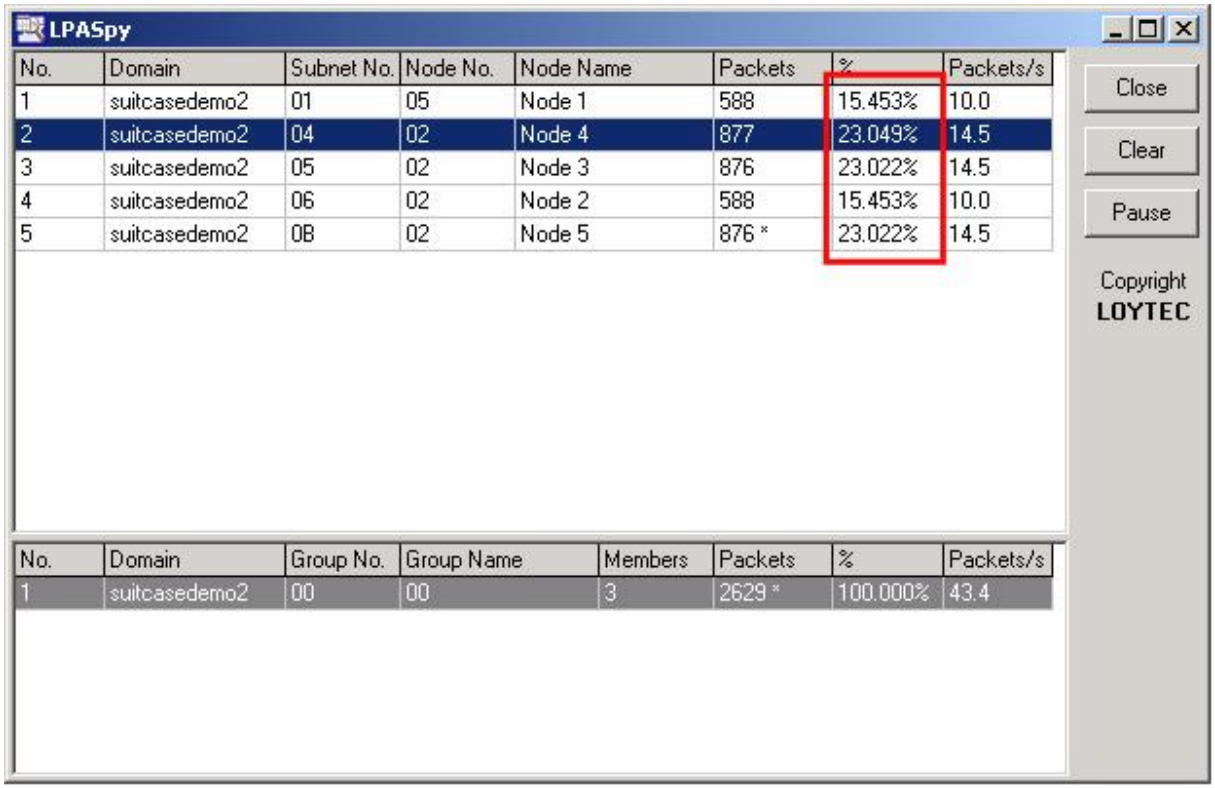

Abbildung 3: LPASpy Fenster

Bei der Netzwerkanalyse ist es wichtig zu beachten, dass sich Werte für die Kanalauslastung, Fehlerzähler und auch der Missed Preamble Zähler immer auf ein einzelnes Netzwerksegment beziehen. Router und Switches, die die Netzwerksegmente untereinander verbinden, filtern den Datenverkehr in Abhängigkeit der Zielpakete der Daten und verwerfen alle Pakete, die keine korrekte Checksumme aufweisen. Daher ist es in der Regel nicht ausreichend, nur einen einzelnen Kanal zu analysieren, sondern erforderlich, alle problembehafteten Kanäle gesondert zu betrachten. In manchen Fällen kann es darüber hinaus erforderlich sein, ein und denselben Kanal an mehreren verschiedenen Stellen zu analysieren, da Signal- und Störamplituden auf Grund der Dämpfung des Kabels ortsabhängig sind.

3.2 Netzwerkfehlerrate

Das Statistikfenster zeigt auch Zähler für fehlerhafte Pakete (bad packets) und Netzwerkfehler auf den Karteireitern „General“ und „Error“ an. In Netzwerken mit hoher Kanalauslastung können Fehlerraten bis zu 1% toleriert werden. Powerline Kanäle weisen in der Regel höhere Fehlerraten auf. Liegt der gemessene Fehlerwert wesentlich über diesen Werten so müssen weitere Untersuchungen angestellt werden. Die auf der Seite „Errors“ angezeigten Fehlerzähler geben den Teil des Pakets an, in dem ein Fehler detektiert wurde. Obwohl diese

Information – da das Paket ja verfälscht wurde – nicht absolut zuverlässig ist, ist es oft möglich, auf Grund der Absenderadresse der Pakete Rückschlüsse auf die Ursprungsknoten der fehlerhaften Pakete zu ziehen. Diese Information kann dazu verwendet werden, den Netzwerkpfad zu den fehlerhaften Knoten zu ermitteln. Das Netzwerkfehler-Statistikfenster ist in Abbildung 4 zu sehen.

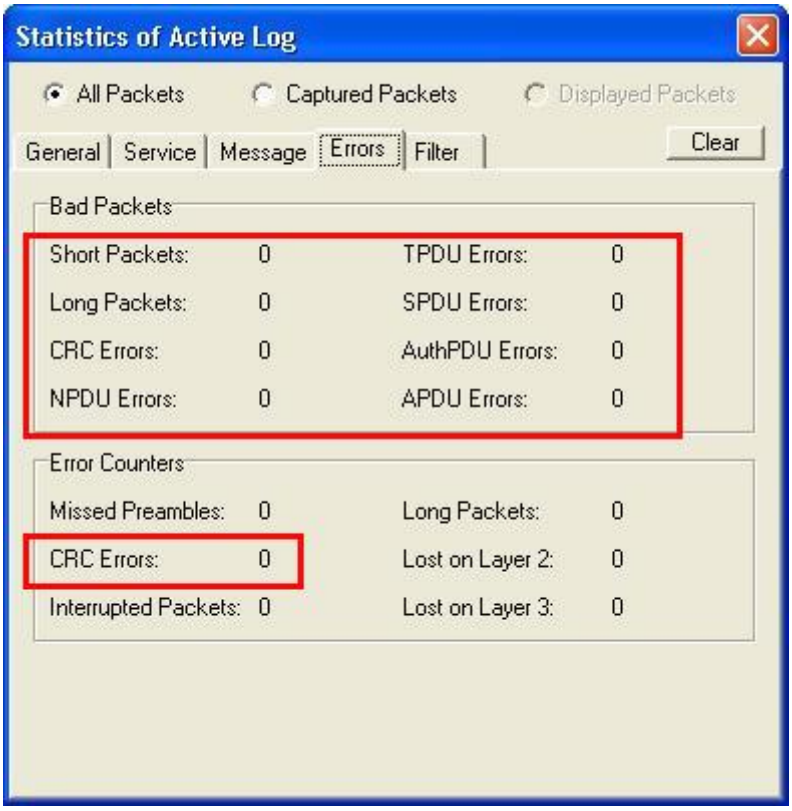

Abbildung 4: Fehlerstatistik im LPA

3.3 Missed Preamble Zähler

Ein weiterer aussagekräftiger Indikator für den Netzwerkzustand ist der Missed Preamble Zähler. Diese Zähler wird inkrementiert, wenn der LPA Protokoll Analysator den Beginn eines Paketes (eine Präambel) erkennt, dieser Präambel jedoch kein Paket nachfolgt. Dies wird meist durch Einstreuungen am Netzwerkkabel oder Paketkollisionen ausgelöst. Die Empfindlichkeit des Missed Preamble Zählers ist sehr hoch, daher treten in der Regel auch auf gut funktionierenden Kanälen einige wenige Missed Preables auf. Zählt der Missed Preamble Counter jedoch rasch hinauf (beispielsweise 10-100 Zähler/s auf FT Kanälen), so sind Probleme auf dem Netzwerksegment wahrscheinlich. Frequenzumformer sowie eine fehlende oder fehlerhafte Netzwerkterminierung können solche Probleme verursachen.

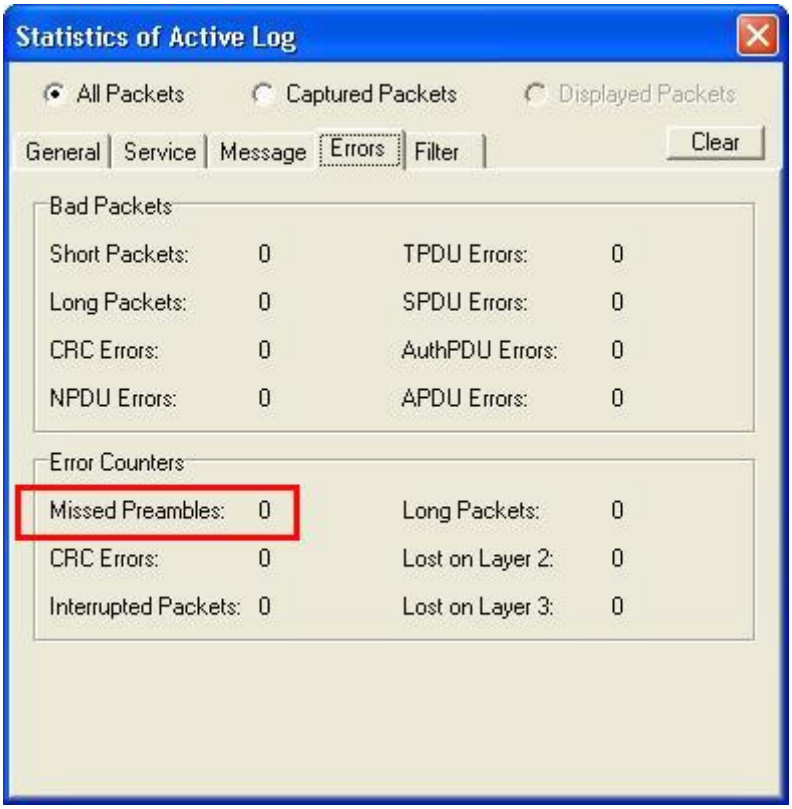

Abbildung 5: Missed Preamble Zähler.

3.4 Check Alternate Pakete

Das Alternate Path Bit in den Paketen kann dazu verwendet werden, nicht erreichbare Knoten oder fehlerhafte Netzwerkverbindungen zu finden. Dieses Bit wird für die letzten beiden Wiederholungen beim Request/Response oder Acknowledged Übertragungsdienst gesetzt, falls der Zielkonten auf die Anfragen nicht antwortet. Daher kann man die Adresse der nicht erreichbaren Knoten ermitteln, indem man mit Hilfe eines Filters alle Pakete mit gesetztem Alternate Path Bit anzeigt. Die Adressen der nicht erreichbaren Knoten sind die Zieladressen dieser Pakete. Abbildung 6 zeigt, wie solch ein Filter erstellt werden kann, um nur Pakete mit gesetztem AP Bit anzuzeigen. Ein vordefinierter Filter für Alternate Path Pakete (only_alternate_path.pft) wird auch mit der LPA Protokollanalysator Software mitgeliefert.

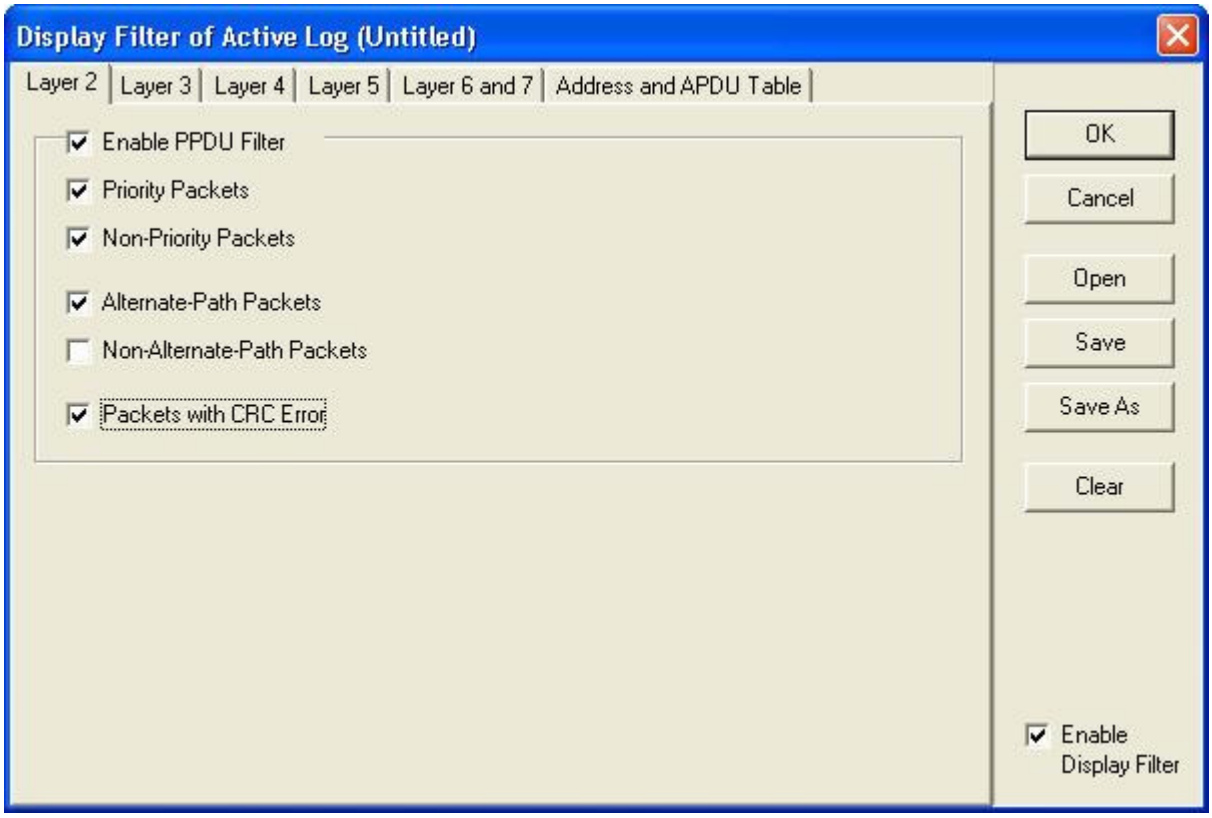

Abbildung 6: Display Filter für Alternate Path Pakete.

Es ist auch interessant herauszufinden, ob Knoten manchmal nicht antworten oder ob diese Knoten nie erreicht werden können. Antwortet ein Knoten auf eine Nachricht, in der das AP Bit gesetzt ist, so ist das AP bit auch in der Antwort (Response oder Acknowledgement) gesetzt.

Nicht erreichbare Knoten deuten auf nicht installierte, nicht funktionierende oder nicht erreichbare Knoten hin. Knoten könnten beispielsweise auf Grund von fehlerhafter Verkabelung, Kanalüberlastung oder defekten Routern nicht erreicht werden. Auch eine falsche Konfiguration der Protokolltimer kann Pakete mit gesetztem Alternate Path Bit verursachen. Die meisten modernen Installationstools verwalten jedoch diese Timer automatisch, sodass dies in der Regel als Fehlerursache ausgeschlossen werden kann.

In all diesen Fällen sollte jedoch überprüft werden, ob die nicht erreichbaren Knoten mit der erforderlichen Spannung versorgt und ordnungsgemäß am Netzwerk angeschlossen sind. Wenn die Spannungsversorgung und der Netzwerkanschluss überprüft sind, muss der Kommunikationspfad zwischen den beteiligten Knoten analysiert werden. Dazu wird der LPA Protokollanalysator an alle Kanalsegmente zwischen den beiden Knoten angeschlossen und die Kanalbandbreitenauslastung und Fehlerrate überprüft.

3.5 Analyse mit dem Oszilloskop

Ein Oszilloskop kann für die Suche nach Verkabelungsproblemen, Interferenzproblemen oder fehlerhafter Terminierung eingesetzt werden. Auf einem ordnungsgemäß temrinierten Bussegment mit FT-10 Transceivern darf die Spannungsamplitude des Datensignals nicht

mehr als 1,5Vpp betragen. Das Rauschsignal am Netwerk sollte im Vergleich dazu gering (max. 10% des Nutzsignals).

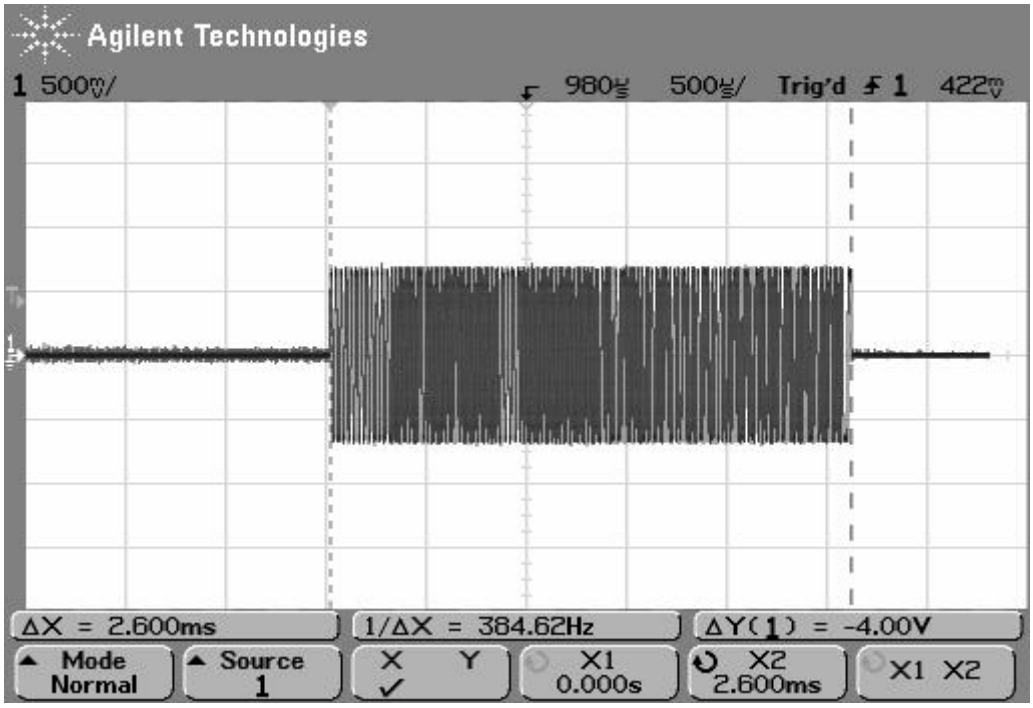

Abbildung 7: Oszilloskopbild eines Pakets auf einem ordnungsgemäß terminierten Kanal.

Signalamplituden >1,5Vpp weisen darauf hin, dass der Kanal nicht ordnungsgemäß terminiert ist (siehe Abbildung 8). Auf Netzwerksegmenten mit großer Kabellänge ist es wichtig, Messungen mit dem Oszilloskop an verschiedenen Positionen durchzuführen, da sowohl das Nutz- als auch das Störsignal der Kabeldämpfung unterliegen und deren Amplituden daher positionsabhängig sind.

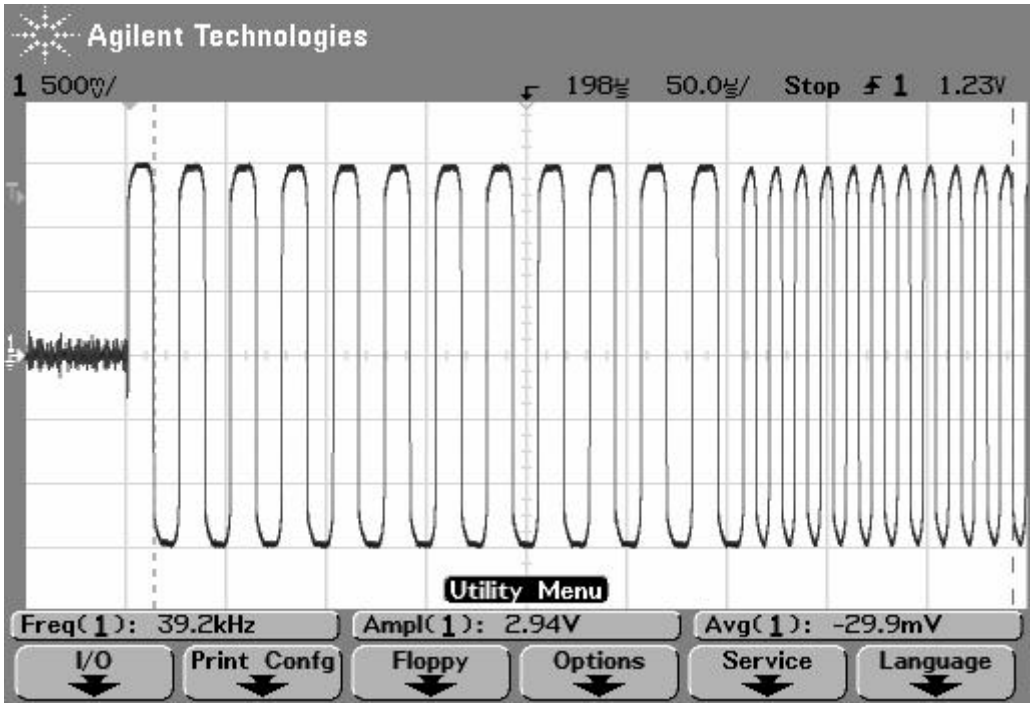

Abbildung 8: Oszilloskopbild eines Pakets auf einem nicht terminierten Kanal.

4 Problembehandlung

Dieser Abschnitt zeigt, wie die gefundenen Probleme effizient behoben werden können.

4.1 Verringern der Netzwerkbelastung

Wenn die Netzwerkanalyse ergeben hat, dass die Netzwerkbelastung zu hoch ist, so muss der Datenverkehr am Netzwerk reduziert werden. Das LPASpy Programm zeigt an, ob einzelne Knoten für den hohen Datenverkehr verantwortlich sind oder ob der gesamte Netzwerkverkehr die Annahmen, die beim Design des Systems gemacht wurden, übersteigt. Oftmals trägt die Gebäudeleittechnik wesentlich zur Netzwerkbelastung bei. Wesentliche Verbesserungen können zumeist erzielt werden, wenn man die Pollingintervalle des Visualisierungssystems vergrößert und die Datenpunkte entsprechend ihrer Funktion in Gruppen unterteilt. Diesen Gruppen können dann (beispielsweise bei OPC Servern) unterschiedliche Updateintervalle zugewiesen werden. So sind in der Regel die Werte für Lichtsteuerungen wesentlich zeitkritischer als jene Werte, die zur Temperaturregelung verwendet werden. Abhängig von der Knotenapplikation können oft auch Parameter wie minimale Updateraten oder send-on-delta Einstellungen eine Verringerung der Netzwerkbelastung ermöglichen.

Bei gruppenadressierten Nachrichten in Gruppen mit mehr als 3 Gruppenteilnehmern sollte der Übertragungsdienst „Unacknowledged Repeated“ anstelle von „Acknowledged“ verwendet werden. Dadurch wird die Netzwerkbelastung bei gleichzeitiger Beibehaltung der Zuverlässigkeit der Datenübertragung verringert.

Wenn mit Hilfe dieser Maßnahmen die gewünschte Netzwerkauslastung nicht erreicht werden kann, so muss die Struktur des Netzwerks überarbeitet werden. Der Applikationshinweise AN007 [1] enthält allgemeine Hinweise und Richtlinien für die Strukturierung von Netzwerken.

4.2 Beheben von Verkabelungsproblemen

Missed preambles und Netzwerkfehler werden zumeinst von Einstreuungen, fehlenden Abschlusswiderständen oder Kabelbrüchen hervorgerufen. In all diesen Fällen ist es wichtig, möglichst die Fehlerursache zu beheben und nicht nur die Symptome zu bekämpfen. Fehlende Abschlusswiderstände können, wie in den vorangegangenen Kapiteln beschrieben, mit Hilfe eines Oszilloskops gefunden werden. LOYTEC bietet Terminatoren für TP/XF-1250 und FT Kanäle (Bus und Freie Topologie) zur Hutschienenmontage an.

Abbildung 9: L-Term Netzwerkterminator

Wenn der FT-10 Bus mit Abschlusswiderständen versehen ist, die gemessene Signalamplitude jedoch 1,5Vpp übersteigt, so liegt wahrscheinlich ein Kabelbruch oder ein Kontaktproblem bei einer der beiden Netzwerkadern vor.

Bei EMV Problemen ist es wichtig, die Verursacher der Störung zu finden. Frequenzumformer stellen dabei eine häufige Quelle dar. Stellen Sie sicher, dass die Installationsanleitungen der Hersteller korrekt eingehalten wurden. Falls das Problem weiterhin besteht, wenden Sie sich an die Hersteller der die Störung verursachenden Geräte.

In Fällen in denen die Störungsursache nicht behoben werden kann, hilft es manchmal, Router oder Switches in den Kanal einzufügen. Da diese Geräte die Checksumme jedes Pakets überprüfen, werden auf diese Weise zerstörte Pakete und Netzwerkstörungen gefiltert. Speziell der Smart-Switch-Modus des L-Switches leistet für derartige Anwendungen gute Dienste, da dieser zum Netzwerk ohne Umkonfiguration hinzugefügt und so die Wirkung dieser Maßnahme unmittelbar beobachtet werden kann.

5 Glossar

Dieser Abschnitt definiert die in diesem Dokument verwendete Fachbegriffe.

- Ein **Netzwerk** (Network) beinhaltet alle Knoten in einem Projekt. Ein Netzwerk kann aus mehreren Domains bestehen.

- Ein **Gerät** (Device) ist ein einzelner Knoten in einem Netzwerk. Ein Gerät kann Anwendungen (z. B. Lichtsteuerung, Klimasteuerung,…) abarbeiten. Auch Netzwerkinfrastrukturkomponenten sind Geräte. Ein Gerät kann mehrere Netzwerkanschlüsse (Ports) haben.

- Ein **Netzwerkanschluss** (Port) stellt die Verbindung zu einem Netzwerkkanal her. Netzwerkinfrastrukturkomponenten können mehrere Netzwerkanschlüsse haben, so dass mehrere verschiedene Kanäle an das Geräte angeschlossen werden können. Applikationsknoten haben typischerweise nur einen Netzwerkanschluss.

- Eine **Domäne** (Domain) beschreibt alle Knoten, denen die selbe Domain ID zugeordnet ist. Eine gemeinsame Domäne wird allen Knoten in einem LNS Projekt zugeordnet. Eine Domain kann bis zu 32385 Knoten enthalten.

- Ein **Subnetz** (Subnet) beschreibt alle Knoten die dieselbe logische Subnetzadresse und Domänenadresse zugeordnet haben. LNS weist jedem Kanal (Channel) ein eigenes Subnetz zu. Subnetze dürfen sich nicht über mehrere Anschlüsse von Configured Router Geräten erstrecken. Eine einzelne Domäne kann bis zu 255 Subnetze haben.

- Ein **Knoten** (Node) ist die logische Repräsentation eines Netzwerkanschlusses. Jeder Knoten hat eine eigene Domaintabelle, Adresstabelle und Netzwerkvariablentabellen und eine weltweit eindeutige Node ID. Ein einzelnes Gerät, das mehrere Netzwerkanschlüsse hat (z. B. L-Proxy Gateway) repräsentiert am Netzwerk mehrere Knoten, wobei jeder Knoten separat kommissioniert werden muss.

- Ein **Netzwerksegment** (Network Segment) beschreibt ein physikalisches Segment des Netzwerks. Netzwerksegmente sind untereinander durch Router, Switches oder Repeater verbunden. Ein Netzwerksegment kann als das “Kabel zwischen Netzwerkinfrastrukturkomponenten” betrachtet werden. In Abhängigkeit vom Transceivertyp, der auf dem Kanal verwendet wird, darf nur eine beschränkte Anzahl von Geräten auf einem Netzwerksegment betrieben werden. Beispielsweise dürfen auf einen TP/FT-10 Kanal maximal 64 Geräte pro Netzwerksegment angeschlossen werden.

- Ein **Kanal** (Channel) fasst alle Knoten auf einem Kabelsegment zusammen. Kanäle können durch Router, Switches oder Repeater untereinander verbunden werden. LNS ordnet jedem Channel eine eigene Subnetznummer zu. Jedem Kanal wird auch ein Kanaltyp zugeordnet. Der Kanaltyp legt fest, welchen Transceiver die an den Kanal angeschlossenen Geräte zur Datenübertragung verwenden müssen. Verschiedenen Kanaltypen sind in den LonMark Layer 1-6 Interoperability Guidelines [1] definiert.

- Ein **Transceiver** ist die physikalische Schnittstelle, die einen Netzwerkanschluss an das Netzwerk anbindet. Ein Transceiver muss die Spezifikation für den jeweiligen Kanaltyp erfüllen.

- **Kanaltypen**:

  - **TP/FT-10**: Ein Kanal, dessen Knoten einen Transceiver gemäß der EIA709.3 Spezifikation (z. B. FTT-10A) verwenden.

  - **TP/XF-xxx**: Ein Kanal, dessen Knoten den TP/XF-xxx Transceiver im Standard Modus verwenden. xxx beschreibt die verschiedenen Bitraten, z. B. TP/XF-1250 für einen 1250kbit/s Kanal.

  - **Kollisionsfreier TP/XF-1250 Kanal** (Collision-less TP/XF-1250): Ein Hochgeschwindigkeitskanal, der die elektrischen Spezifikationen des TP/XF-1250 Kanals benutzt, den Buszugriff jedoch über einen kollisionsfreien Hochgeschwindigkeitsalgorithmus abwickelt.

  - **IP-852**: Ein Kanal, der Geräte mit einer Ethernetschnittstelle gemäß dem Standard EIA-852 verbindet. Die Adressinformationen aller Kanalteilnehmer werden von einem Konfigurationsserver (Configuration Server) verwaltet. In LNS Projekten werden für IP-852 Kanäle die Bezeichnungen IP-10L und IP-10W verwendet. Der IP-10L Kanal sollte für lokale IP Netzwerke (LAN) verwendet werden, der IP-10W Kanal hingegen für Kanäle, die sich über entfernte IP Netzwerke (WANs) erstrecken. LNS verwendet diese unterschiedlichen Kanaltypen, um die Protokolltimer entsprechend den typischen Kanalverzögerungszeiten einzustellen. Andere gebräuchliche Namen für IP-852 Kanäle sind “CNIP Kanäle”.

  - **TP-RS485-xxx**: Ein Kanal, auf dem der TP-RS485 Transceiver verwendet wird. xxx beschreibt die unterschiedlichen Bitraten, z. B. TP-RS485-39 oder TP-RS485-78 für 39kbit/s bzw. 78 kbit/s Kanäle.

- Ein **Router** ist ein Netzwerkinfrastrukturprodukt, das mit mehreren Netzwerkanschlüssen ausgestattet ist. Er leitet die empfangenen Datenpakete auf Grund von konfigurierten Routing-Tabellen weiter. Die Tabellen müssen bei der Installation des Netzwerks und bei Änderungen an der Netzwerkstruktur vom Netzwerkmanagementprogramm in die Router geschrieben werden. Im Configured Router Modus des L-IP Router und L-Switch XP Router wird die Routing-Tabelle während der Installation vom Netzwerk Management Tool konfiguriert.

- Ein **Smart Switch** ist ein Netzwerkinfrastrukturprodukt, das mit mehreren Netzwerkanschlüssen ausgestattet ist. Es leitet die empfangenen Datenpakete auf Grund einer internen Switching-Tabelle weiter. Im Smart Switch Modus des L-IP Router und L-Switch (XP) Router werden die Switching-Tabellen durch eine Analyse der Adressen in den empfangenen Datenpaketen selbständig gelernt. Die Switching-Tabellen müssen daher nicht von einem Netzwerkmanagementprogramm konfiguriert werden.

- **SCADA** steht für ‘Supervisory Control and Data Acquisition’. Ein SCADA System läuft zumeist auf einem PC und ist mit einer grafischen Oberfläche zur Überwachung und Steuerung der Geräte in einem Netzwerk ausgestattet. SCADA Systeme werden auch oft als Gebäudemanagementsysteme oder Building Management Systeme (BMS) bezeichnet.

- **BMS** ist die Abkürzung für ‘Building Management System’. Ein BMS System läuft zumeist auf einem PC und ist mit einer grafischen Oberfläche zur Überwachung und Steuerung der Geräte in einem Netzwerk ausgestattet. BMS Systeme werden auch oft als Gebäudemanagementsysteme oder SCADA Systeme bezeichnet.

6 Referenzen

[1] LOYTEC electronics GmbH: Applikationshinweise AN007G Netzwerkinfrastruktur Whitepaper, Dokument Nummer 86001301

[2] D.Loy, D. Dietrich, H.J. Schweinzer: LON-Technologie, Hüthig Buch Verlag Gmbh, Heidelberg, 1998