1 Network Troubleshooting White Paper

This application note gives tips and hints for troubleshooting EIA 709 networks. It describes a way how to use LOYTECs LPA Protocol Analyzer to track down problems efficiently.

2 Network Troubleshooting Workflow

Successful and time efficient troubleshooting is based on a structured workflow. A recommended approach is shown in Figure 1.

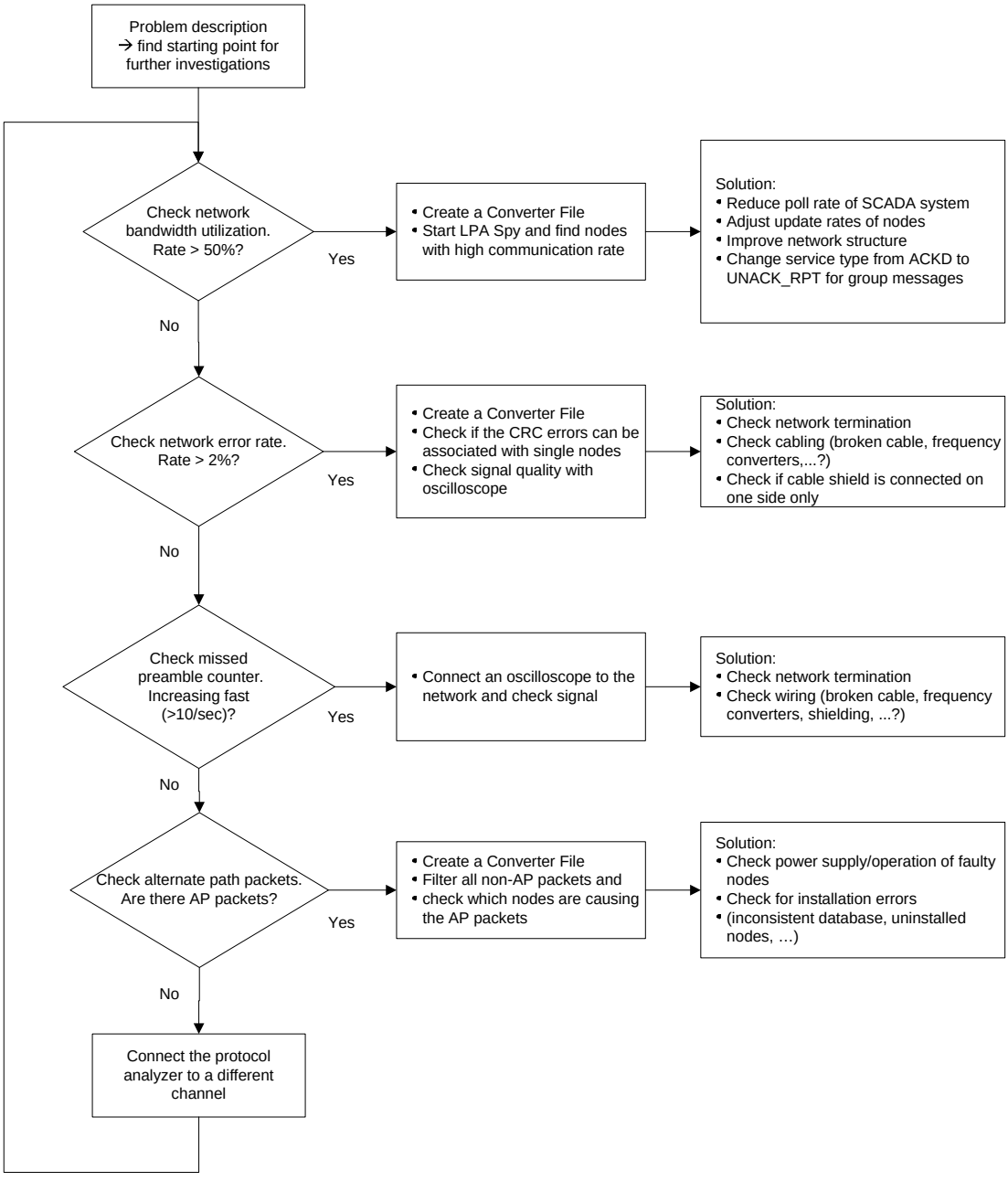

Figure 1: Workflow for troubleshooting EIA 709 networks

2.1 Problem Description

At the beginning of each network analysis, it is important to get an overview of the problems in the network. Instead of connecting the LPA Protocol Analyzer to the network and collecting lots of data, it is highly recommended to discuss the network problems with the local engineers. This gives a good overview about the problem and often provides information where to start the investigations on the network.

Important questions are:

1. ***What is the problem*** *on the network? What are the effects?*

   Are there communication problems on the network? Can some nodes not be contacted by the SCADA system? Are nodes going "offline" in the management tool?

2. ***Which parts of the network*** *are affected?*

   Are there problems with the whole network or only with single network segments or even single nodes?

3. ***When*** *does the problem occur?*

   Is the problem present all the time or only at special occasions? (E.g. at special times, in special situations,…)

4. ***How*** *is the* ***network structured****?*

   Are there backbone channels? Which channel types are used? How many nodes are on the network segments? In most cases it is helpful to have a drawing of the network structure and to mark the "points of trouble" in the drawing.

5. ***What*** *is the* ***communication rate*** *on the network?*

   Which nodes are communicating to each other? Is there a SCADA system which polls the nodes? What is the expected communication rate on the different network channels?

6. *Have there been any* ***changes on the network****?*

   Was the network already running without problems before? Have there been any changes on the network before the time the problems occurred?

This information can be used to find a good start for a first hands-on network investigation. Also the built-in diagnostic features of LOYTEC network infrastructure components can give a good starting point for a network investigation. Monitoring the diagnostic LEDs on L-Switch and L-IP devices, faulty channels can be detected by a red flickering LED. It is recommended to take a closer look at these channels with the LPA Protocol Analyzer.

3 Network Analysis

The collected information must be evaluated to decide at which location in the network the LPA Protocol Analyzer is connected first. If only single nodes in the network are affected, the protocol analyzer should be connected to the channels of these nodes. Communication problems between the nodes and a SCADA system can be investigated by connecting the protocol analyzer to the channel of the SCADA station. The backbone channels of the network can be a good starting point for further investigations if the problem analysis gives no hint where the error is located.

3.1 Check Bandwidth Utilization

The network statistics window gives an overview on the health state of a network channel. The statistics window is opened with the statistic button or via the menu "Packet → Statistics" while the log is running. The first parameter to check is the network bandwidth utilization on the "General" tab of the statistics window (see Figure 2).

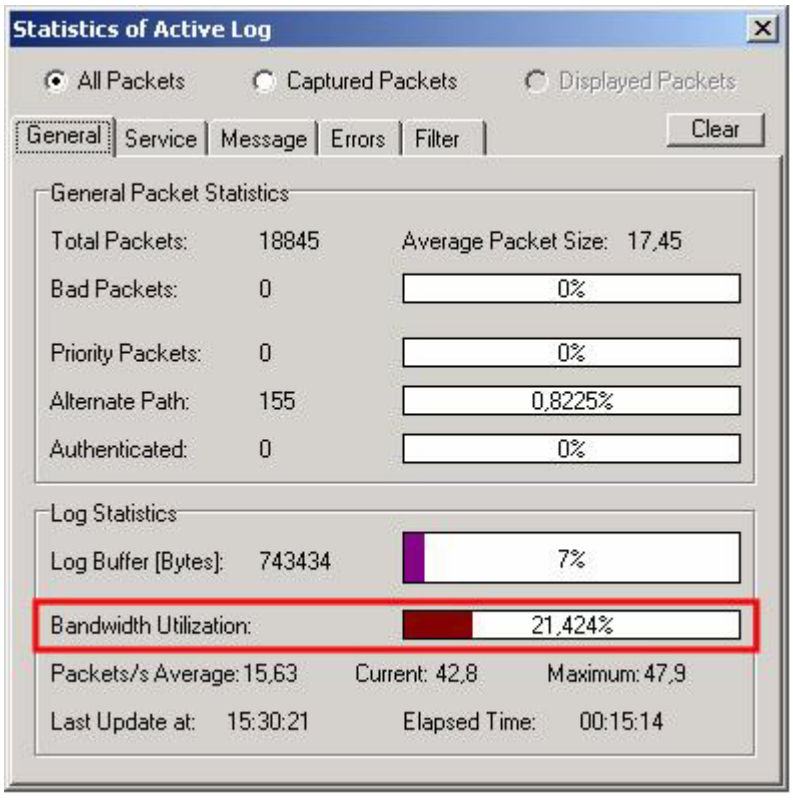

Figure 2: Bandwidth Utilization Statistics.

The network bandwidth utilization should not exceed approx. 50%. Higher bandwidth utilizations need further investigations, which nodes are causing the network traffic. To identify nodes on the network, the LPAConv LNS Plugin can be used to create an LPA converter file from an existing LNS database. The converter file converts network addresses to human readable node names, as specified in the LNS project. The LPASpy tool also uses these names to display the network data (see Figure 3). It can be used to collect data on how much of the network bandwidth is occupied by which node.

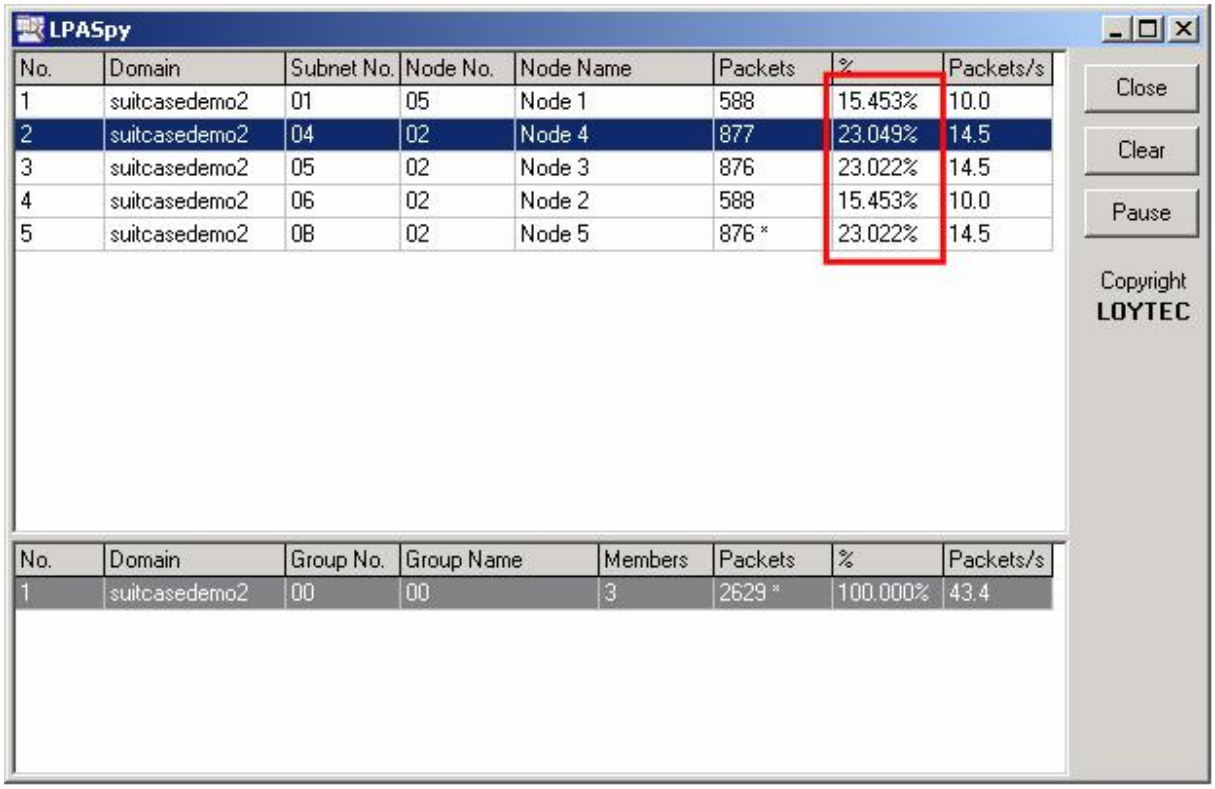

Figure 3: LPASpy dialog.

It is important to realize that the channel load, all errors, and also missed preambles are always related to a single network segment. Routers and Switches, which are interconnecting the network segments, filter network errors and network traffic, depending on the destination addresses of the packets. Therefore it is not sufficient to investigate a single channel. Further, all problematic channels must be investigated separately. In some cases even the same channel has to be investigated from different places, since the signal and noise amplitudes are location dependent.

3.2 Check Network Error Rate

The statistics window also contains counters for bad packets and network errors on the "General" and "Error" tab of the statistics window. On networks with high bandwidth utilization, bad packet rates between 0.5% and 1% can be tolerated. Power line channels usually have even higher error rates. If the error rate significantly exceeds these limits, further investigations have to take place. The listed error types in the "Error" tab indicate the part of the packet where the error was detected. Although the displayed information is not highly reliable, it is often possible to identify addresses of source nodes which send out the faulty packets. This information can be used to follow the network path to the source nodes. The network error statistics window is shown in Figure 4.

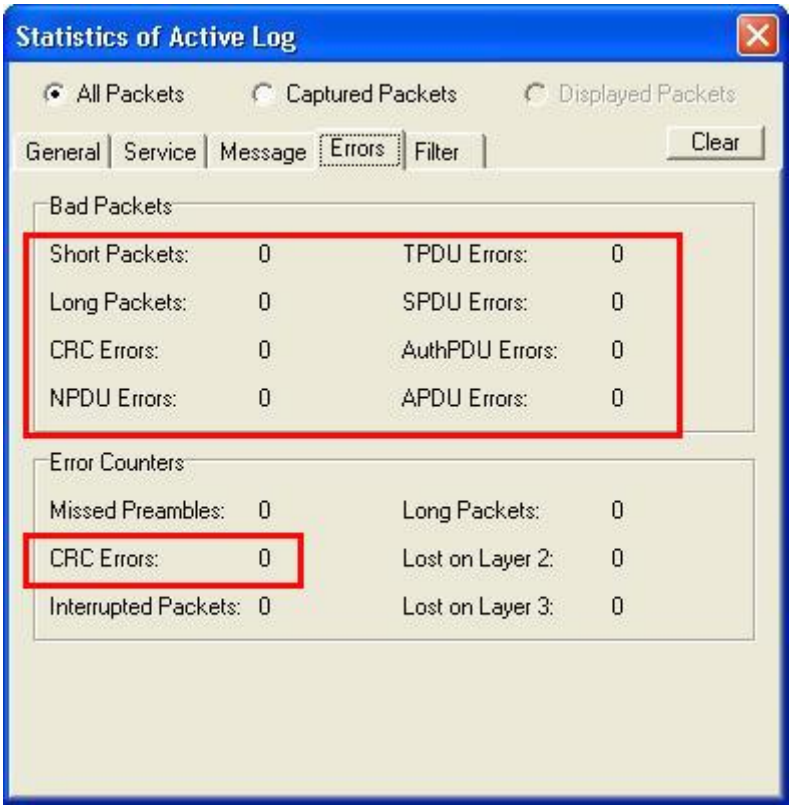

Figure 4: Error Statistics in LPA.

3.3 Check Missed Preamble Counter

Another valuable indicator for network problems is the missed preamble counter. The missed preamble counter is incremented whenever a packet preamble is detected without an actual packet following. In most cases this is caused by noise or packet collisions on the network. The missed preamble counter is quite sensible, so it is common to have a few missed preambles on the channel. If the missed preamble counter counts up quickly (e.g.10-100 counts/sec on FT channels), it is likely that there are problems on the channel. Frequency converters or similar devices as well as missing network terminators may cause such problems.

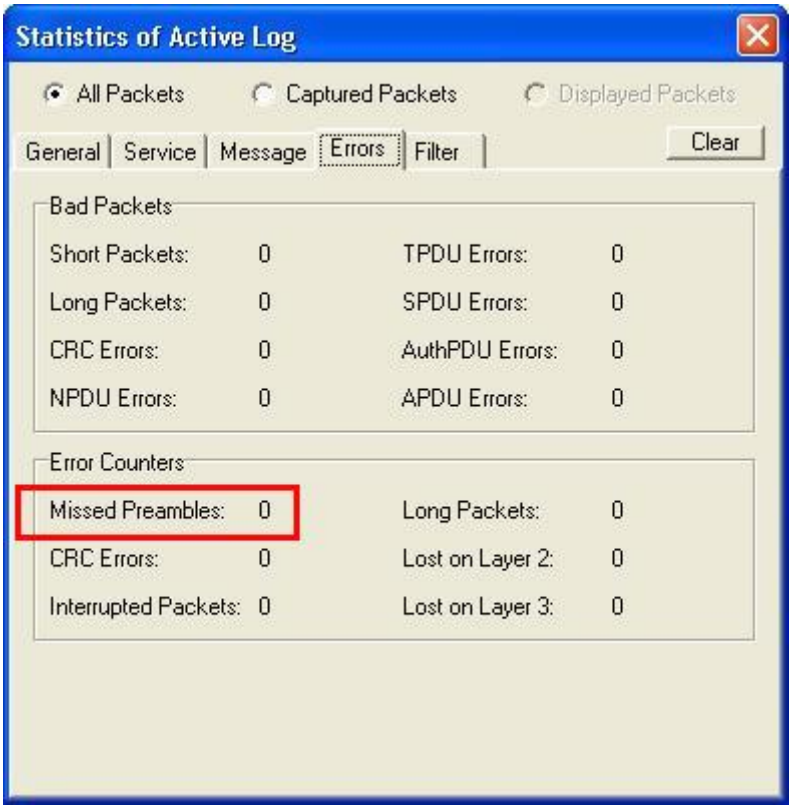

Figure 5: Missed Preamble Counter.

3.4 Check Alternate Path Packets

The Alternate Path Bit of the network packets can be used to find unreachable nodes or nodes with faulty network connections. The Alternate Path bit is set in the last two repeats of request-response or acknowledged transactions in case the destination node is not responding. This means that, when filtering on packets with alternate path bit set, the destination address of the packets are the nodes which can not be reached. Figure 6 shows how to create a display filter in the LPA so that only packets with the AP bit set are displayed. A predefined filter file for alternate path packets (only_alternate_path.pft) is also shipped with the LPA Protocol Analyzer.

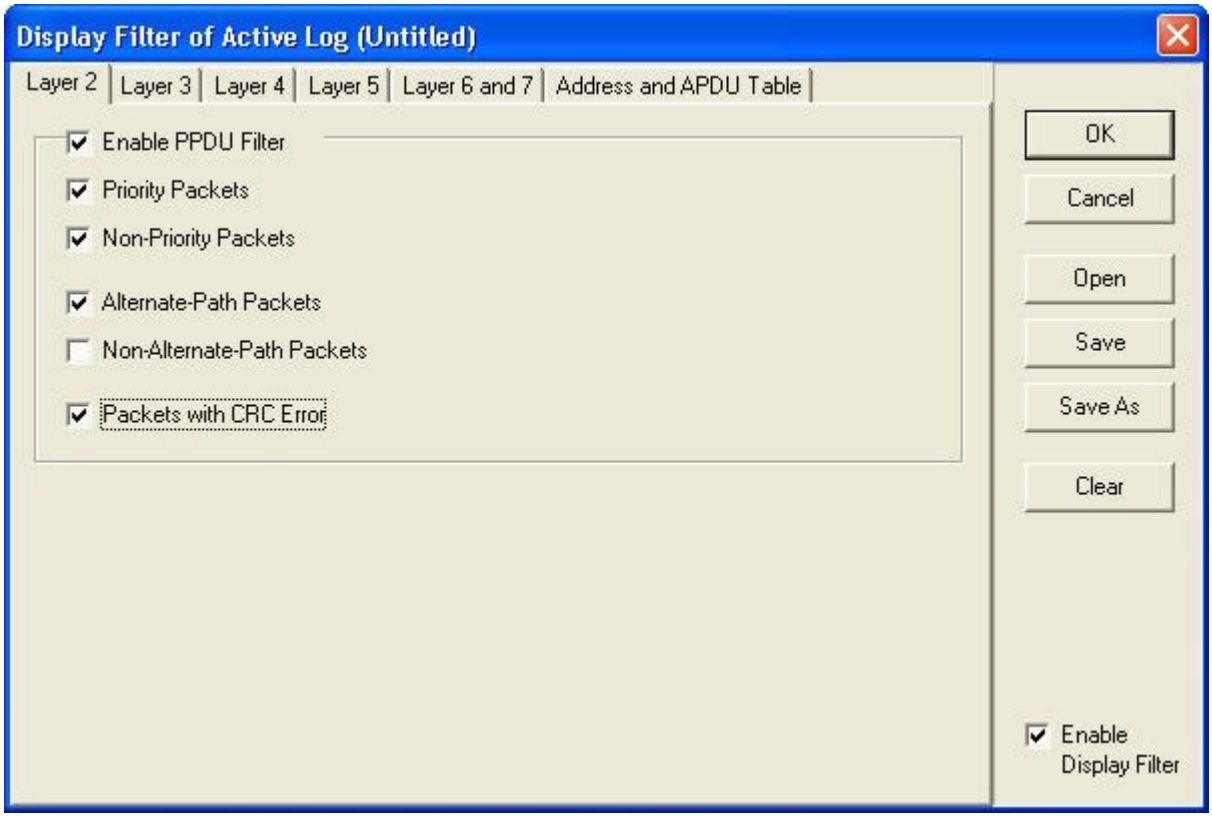

Figure 6: Display Filter for Alternate Path Packets.

It is also interesting to find out if the nodes are only failing to respond sometimes or if they do not respond at all. If the node is responding to an alternate path packet, the response also has the alternate path bit set.

Non-responding nodes sometimes indicate not installed nodes, not working nodes or also nodes, which cannot be reached because of defective routers, faulty cabling or channel overload situations in certain network segments. Also bad timer configuration in the nodes can cause alternate path packets, but most installation tools handle the protocol timers automatically so that the engineer does not have to deal with the timer configuration. In all cases it is important to check if the defective nodes are properly powered and connected to the network. If power and wiring is OK, the network path between the communicating nodes must be checked. To do this, connect the LPA on every channel between the two communicating nodes and check the network bandwidth and error rate on that channel where the packets are lost.

3.5 Analysis with Oscilloscope

An oscilloscope is a useful tool to find the sources for wiring problems, interference or faulty termination. On a properly terminated FT-10 channel the peak-peak amplitude must not exceed 1.5V. The noise on the network must be low (max. 150mV peak-peak amplitude) compared to the signal.

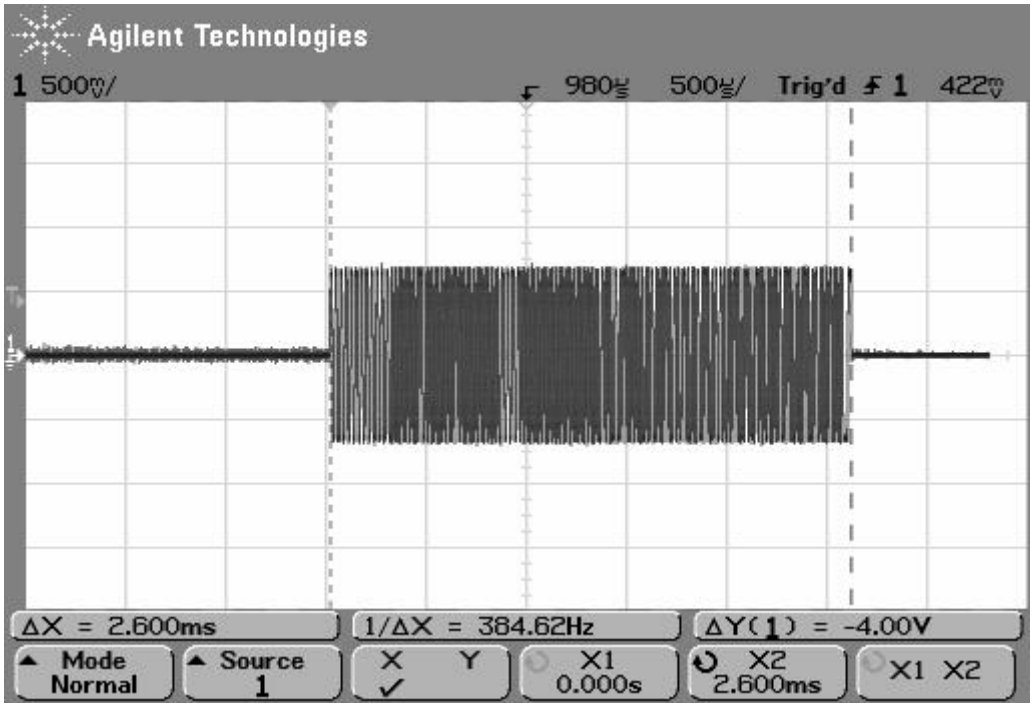

Figure 7: Oscilloscope Screenshot of Packet on properly terminated channel.

It the signal amplitude exceeds 1.5V, the channel probably is not correctly terminated (see Figure 8). On long network segments it is important to take the oscilloscope measurements on several different places because the insertion loss of the cables are lowering the amplitude of both, the packet signal and the noise.

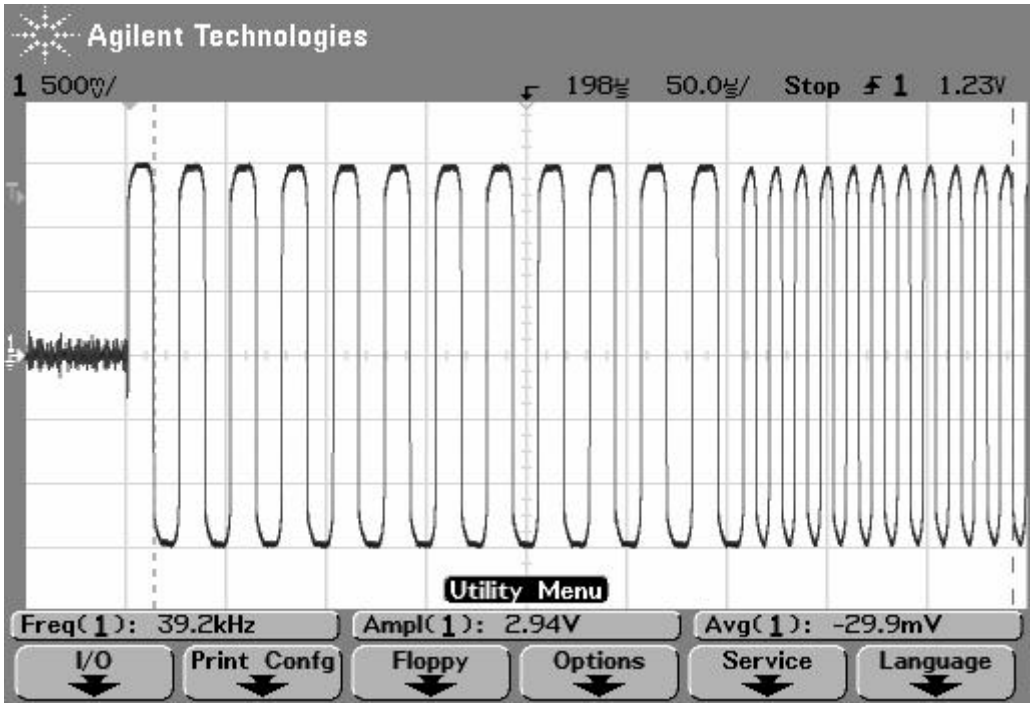

Figure 8: Oscilloscope Screenshot of Packet with missing network termination (Vpp > 1.5V).

4 Problem Solution

This section describes how problems can be solved once they have been identified.

4.1 Reduce Network Load

If the network analysis showed that the network bandwidth utilization is too high, the network communication on the network channels has to be reduced. The LPASpy tool shows if a single node produces the main traffic or if the general communication rate exceeds the assumptions made during the system design.

Often the high network traffic is caused by the SCADA system. To reduce the traffic, sometimes polling intervals can be raised. It is also useful to combine the data points into groups which need to be updated often (e.g. light controllers) and groups which do not need high update rates (e.g. room temperature sensors).

Depending on the node's application it is possible to tune the minimum update rates or send-on-delta values to reduce the network traffic.

For group addressed communication with more than 3 group members it helps to change the communication type from acknowledged to unacknowledged repeated service. This reduces the network traffic caused by the acknowledgement packets but keeps the reliability for the data transmission on the same level.

If it turns out that all these steps are not sufficient for a significant reduction of the network bandwidth utilization, the network has to be redesigned and a proper network structure, using router and switches, must be introduced. Application note AN007 [1] gives a detailed overview on how to structure large networks using high speed backbone channels.

4.2 Fix Cabling Problems

Missed preambles and network errors are mostly caused by interference, missing network terminators or broken cables. In this case it is always important to focus on eliminating the source of the problem (if possible) rather than reducing the symptoms. Missing terminators can be detected with an oscilloscope as described above. LOYTEC offers DIN-Rail mountable terminators for TP/XF-1250 channels and FT channels (bus and free topology).

Figure 9: L-Term Network Terminator

If terminators are present on the network but the oscilloscope shows signal amplitudes above 1.5V peak-to-peak, it is very likely that one of the two cables on the network segment are broken or not properly connected.

For interference problems, the source of the problem must be detected. Frequency converters are a good starting point for the investigations. Make sure that the installations exactly follows the installation instructions of the device vendors. If the problems persist, contact the vendor of the faulty device.

In situations where the source of the interference problem can not be eliminated, it might help to insert routers or switches in the network channel. Since these devices are performing a CRC check on every packet, they are filtering out bad packets and network noise. Especially the smart switch mode of the L-Switch devices is useful in that case because the device can be installed without doing any reconfiguration in the network management tool. It immediately becomes clear whether the L-Switch device improves the situation or not.

5 Glossary

This section defines the terms used in this document:

- A **Network** contains all nodes in an installation. A network can consist of multiple Domains, Segments or Channels.

- A **Device** describes a single unit in the network. A device can run an application, e.g. light controller, HVAC controller. Also network infrastructure components are devices. A single device can have multiple ports connecting to different Segments

- A **Domain** describes a collection of nodes, which have assigned the same domain ID. A single domain is assigned to each LNS project.

- A **Subnet** describes a collection of nodes which have the same logical subnet and domain address. LNS assigns a single subnet to each channel. Subnets must not be used across different ports of configured routers. A single domain can have up to 255 subnets.

- A **Node** is a logical representation of a port. Every node has assigned its own domain table, address table and NV tables and has a world wide unique Node ID. A single device which has multiple ports (like e.g. L-Proxy) also represents multiple nodes, where every node has to be commissioned separately in the network.

- A network **Segment** describes a physical segment of the network. Multiple network segments are connected by routers, switches, or repeaters. Thus, a network segment is "the piece of cable between multiple network infrastructure products" to which the node on the segment are connected. Depending on the transceiver type used on the channel, a limited number of nodes can be connected to the network segment. E.g. for TP/FT-10 nodes, the maximum node count per network segment is 64 (including the network infrastructure products).

- A **Channel** is a logical collection of nodes. Channels are connected by routers, switches or repeaters. LNS assigns a Subnet number to each channel, if the channel is separated by routers. Each channel has assigned a channel type, which describes the communication parameters, which are used by the transceivers to communicate on the channel. Standard channel type is defined in the LonMark Layer 1-6 interoperability guidelines.

- A **Transceiver** is the physical interface which connects a port to the network. A transceiver must meet the specifications for a specific channel type.

- **Channel types**:

    - **TP/FT-10**: A channel with nodes using the EIA709.3 transceiver (e.g. FTT-10A).

    - **TP/XF-xxx**: A channel which uses the TP/XF transceiver in standard mode. Xxx defines different bit rates, e.g. TP/XF-1250 for a 1250kbit/s channel.

  - **IP-852**: A channel which connects devices with an IP interface according to the EIA-852 standard. The address information of all channel members is managed by a configuration server. In LNS projects, the names IP-10L and IP-10W are used for IP-852 channel. The IP-10L channel should be used for local IP networks (LANs), whereas the IP-10W channel is used for wide area IP networks (WANs). LNS uses these channel type specification to adjust the protocol timers correctly. Other names for IP-852 channels, which are sometimes used, are "CNIP channels" or LonWorks/IP channels.

- A **Router** is a network infrastructure product, which is equipped with multiple ports. It forwards the packets to specific ports because of the information in an internal routing table. In configured routing mode of L-IP and L-Switch XP, the routing table is configured during the installation process by the network management tool.

- A **Smart Switch** is a network infrastructure product, which is equipped with multiple ports. It forwards the packets to specific ports because of the information in internal switch table. In smart switch mode of L-IP and L-Switch XP, the switch table is learned from the network traffic. There is no need to configure the table in a network management tool.

- **SCADA** stands for 'Supervisory Control and Data Acquisition'. It often runs on a PC and includes a graphical representation of the network to monitor and control nodes on the network. Sometimes the term BMS is used for SCADA systems.

- **BMS** stands for 'Building Management System'. It often runs on a PC and includes a graphical representation of the network to monitor and control nodes on the network. Sometimes the term 'SCADA' is used instead of BMS.

6 References

[1] LOYTEC electronics GmbH: Application Note AN007E Network Infrastructure Whitepaper, Document Number 86001201

[2] D.Loy, D. Dietrich, H.J. Schweinzer: Open Control Networks, Kluwer Academic Publishers, 2001