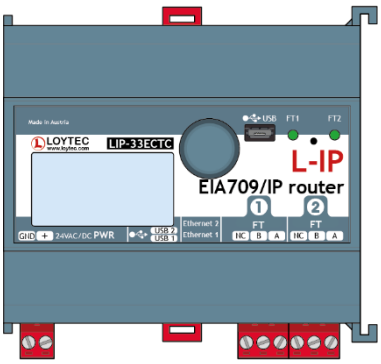
L-IP™

CEA-709/IP Router

Benutzerhandbuch

Delta IBT (Europe) GmbH



Kontakt

Delta Intelligent Building Technologies (Europe) GmbH
Blumengasse 35
1170 Wien
ÖSTERREICH
support@loytec.com
http://www.loytec.com

Version 8.6.0

Dokument № 88066020

DELTA IBT (EUROPE) GIBT KEINE UND SIE ERHALTEN KEINE GARANTIEN ODER ABMACHUNGEN, WEDER AUSGESPROCHEN, NOCH UNAUSGESPROCHEN, WEDER SATZUNGSGEMÄß NOCH IN IRGENDEINER KOMMUNIKATION MIT IHNEN, UND DELTA IBT (EUROPE) LEHNT JEGLICHEN ANSPRUCH AUF UNAUSGESPROCHENE GARANTIEN BEZÜGLICH DER GEBRAUCHSTAUGLICHKEIT ODER TAUGLICHKEIT FÜR IRGENDEINEN BESTIMMTEN GEBRAUCH AB. DIESES PRODUKT IST NICHT DAFÜR KONZIPIERT, IN EINER AUSRÜSTUNG FÜR CHIRURGISCHE IMPLANTATE IM KÖRPER VERWENDET ZU WERDEN, NOCH IST ES DAFÜR KONZIPIERT, IN ANDEREN ANWENDUNGEN, DIE LEBEN UNTERSTÜTZEN ODER ERHALTEN, IN DER FLUGKONTROLLE ODER MASCHINENKONTROLLE INNERHALB DER AUSRÜSTUNG 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. DELTA IBT (EUROPE) ÜBERNIMMT KEINERLEI GARANTIEN FÜR DIE IN DIESEM DOKUMENT GELISTETEN PRODUKTE VON DRITTANBIETERN.

Ohne vorherige schriftliche Einwilligung von Delta IBT (Europe) 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™, LIOB-Connect™, LIOB-FT™, L-IP™, LPA™, L-Proxy™, L-Switch™, L-Term™, L-VIS™, L-WEB™, L-ZIBI™, ORION™ Stack und Smart Auto-Connect™ sind Markennamen von Delta Intelligent Building Technologies (Europe) 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 Einleitung 11
1.1 Übersicht 11
1.1.1 L-IP 11
1.1.2 L-IP Redundant 13
1.2 L-IP Modelle 15
1.3 Umfang dieses Dokumentes 16
2 Haftungsausschluss Cyber-Sicherheit 17
3 Sicherheitshinweise 18
4 Was ist neu im L-IP 24
4.1 Neuigkeiten im L-IP 8.6.0 24
4.2 Neuigkeiten im L-IP 8.4.0 25
4.3 Neuigkeiten im L-IP 8.2.8 26
4.4 Neuigkeiten im L-IP 8.2.0 26
4.5 Neuigkeiten im L-IP 8.0.0 26
4.6 Neuigkeiten im L-IP 7.6.0 27
4.7 Neuigkeiten im L-IP 7.4.0 27
4.8 Neuigkeiten im L-IP 7.2.0 28
4.9 Neuigkeiten im L-IP 7.0.0 30
4.10 Neuigkeiten im L-IP 6.4.0 31
4.11 Neuigkeiten im L-IP 6.1.0 33
5 Quick-Start Anleitung 35
5.1 Hardware Installation 35
5.1.1 L-IP 35
5.1.2 L-IP Redundant 35
5.2 IP Konfiguration eines Client-Geräts 36
5.2.1 Konfiguration auf dem Web-Interface 36
5.2.2 Configuration über das LCD-Display 37
5.3 Konfigurationsserver-Einstellungen 39
5.4 Konfiguration als Drop-In-Ersatz für LON-Router 40
5.5 L-IP Redundant Konfiguration 40
6 Hardware Installation 42
6.1 Gehäuse 42
6.2 Produkt-Label 42
6.3 Montage 44
6.4 Signal LEDs 44
6.4.1 Power LED 44

6.4.2 Status LED ... 44
6.4.3 CEA-709 Activity LED ... 44
6.4.4 Twin Router Status LED (Nur L-IP Redundant) ... 45
6.4.5 Ethernet Link LED ... 46
6.4.6 Ethernet Activity LED ... 46
6.4.7 CEA-852 Status LED (CNIP LED) ... 46
6.4.8 Konfigurationsserver LED ... 46
6.4.9 Wink-Aktion ... 46
6.4.10 Netzwerk Diagnose ... 47
6.5 Statustaster ... 47
6.5.1 Rücksetzen Forwarding Tabellen ... 47
6.6 LCD-Anzeige und Dreh-/Drückrad ... 48
6.6.1 Geräteeinstellung ... 48
6.6.2 Senden einer Node-Pin-Nachricht ... 49
6.6.3 CEA-852 Geräteeinstellung ... 50
6.6.4 Router Mode Einstellung ... 50
6.7 Verkabelung ... 51
6.7.1 L-IP ... 51
6.7.2 L-IP Redundant ... 51
7 Web Interface ... 53
7.1 Geräteinformation und Benutzerkonten ... 53
7.1.1 Inbetriebnahme ... 53
7.1.2 Geräteinformation ... 54
7.1.3 Anmeldung am Gerät ... 55
7.2 Gerätestatistik ... 55
7.2.1 System Log ... 55
7.2.2 IP-Statistik ... 56
7.2.3 CEA-852-Statistiken ... 56
7.2.4 Enhanced Communications Test ... 57
7.2.5 Packet Capture ... 58
7.2.6 Mobilfunk ... 58
7.3 Gerätekonfiguration ... 59
7.3.1 Systemkonfiguration ... 59
7.3.2 Port-Konfiguration ... 60
7.3.3 IP-Konfiguration ... 60
7.3.4 Verwenden mehrerer IP-Ports ... 61
7.3.5 802.1X Port-Authentifizierung ... 62
7.3.6 IP Host-Konfiguration ... 63
7.3.7 Dynamic DNS Konfiguration ... 64
7.3.8 WLAN-Konfiguration ... 65

7.3.9 Mesh-Konfiguration ... 68
7.3.10 VNC-Konfiguration ... 73
7.3.11 CEA-709-Konfiguration ... 73
7.3.12 CEA-852-Gerätekonfiguration ... 74
7.3.13 CEA-709 Router-Konfiguration ... 75
7.3.14 CEA-852 Server-Konfiguration ... 76
7.3.15 CEA-852 Channel List ... 78
7.3.16 SSH-Server-Konfiguration ... 79
7.3.17 SNMP ... 79
7.3.18 VPN-Konfiguration ... 80
7.3.19 LTE-Konfiguration ... 82
7.4 Sicherheit ... 84
7.4.1 Ändern der Passwörter ... 84
7.4.2 Zertifikate Verwalten ... 84
7.4.3 Benutzerverwaltung ... 87
7.5 Dokumentation ... 88
7.6 Wartung ... 89
7.6.1 Konfigurationssicherung und Wiederherstellung ... 89
7.6.2 Firmware ... 90
7.6.3 Dokumentation ... 90
7.6.4 Neustart und Löschen von Daten ... 91
7.6.5 Sicherer Neustart ... 91
7.7 Kontakt und Logout ... 92
8 Betriebsarten des L-IP ... 93
8.1 CEA-709 Router - Operating Modes ... 93
8.1.1 Configured Router Modus ... 93
8.1.2 Smart Switch Mode ... 94
8.1.3 Store-and-Forward Repeater Mode ... 95
8.1.4 Smart Switch Mode ohne Subnet-Broadcast Weiterleitung ... 96
8.2 CEA-852 Betriebsarten ... 96
8.2.1 CEA-852 Gerät ... 97
8.2.2 CEA-852 Konfigurationsserver ... 97
8.3 Firewall und NAT Router Konfiguration ... 100
8.3.1 Automatische NAT-Konfiguration ... 100
8.3.2 Mehrere L-IPs hinter einem NAT-Router: Extended NAT Modus ... 101
8.3.3 Mehrere L-IPs hinter einem NAT-Router: Klassische Methode ... 103
8.4 Multicast Konfiguration ... 103
8.5 Internet Timing Aspekte ... 104
8.5.1 Channel-Timeout ... 105
8.5.2 Channel-Delay ... 105

8.5.3 Escrowing-Timer (Packet-Reorder-Timer) ... 105
8.5.4 SNTP-Zeitserver ... 105
8.6 Erweiterte Themen ... 106
8.6.1 Aggregation ... 106
8.6.2 MD5-Authentifizierung ... 106
8.6.3 DHCP ... 106
8.6.4 Dynamische NAT-Adressen ... 106
8.7 Netzwerk-Buffer ... 107
9 Der L-IP im Netzwerk ... 108
9.1 L-IP agiert als Standard CEA-709 Configured Router ... 108
9.2 L-IP agiert als Smart Switch ... 109
9.3 L-IP agiert als L-Switch ... 109
9.4 Verwendung des L-IP in LNS (LonMaker) Netzwerken ... 110
9.5 L-IP als Netzwerkinterface für LNS Anwendungen ... 110
9.6 Remote-LPA Betrieb ... 113
10 L-IP Redundant ... 115
10.1 Redundanz und Fehlererkennung in CEA-709 Netzwerken ... 115
10.1.1 Ursachen für Kommunikationsfehler ... 115
10.1.2 Herkömmliche Strategien zur Redundanz in CEA-709 Netzwerken ... 116
10.2 L-IP Redundant Betriebsarten ... 116
10.2.1 Bus Loop Monitoring ... 116
10.2.2 Router Redundanz ... 117
10.2.3 Knoten- und Netzwerküberwachung ... 118
10.3 Der L-IP Redundant im Netzwerk ... 119
10.4 Installation ... 119
10.4.1 Installieren des L-IP Redundant Plug-In ... 119
10.4.2 Registering des L-IP Redundant Plug-In ... 122
10.4.3 Einfügen des L-IP Redundant ... 123
10.5 L-IP Redundant Plug-In ... 125
10.5.1 Betriebsmodi ... 125
10.5.2 Übersicht ... 126
10.5.3 Gerätestatus ... 127
10.5.4 Kanalstatistiken ... 129
10.5.5 Alarmlog ... 131
10.5.6 Knotenliste ... 132
10.5.7 Parameter ... 136
10.6 Web Interface ... 139
10.6.1 Status ... 139
10.6.2 Channel Statistics ... 140

10.6.3 Alarm Log ... 141
10.6.4 Node List Configuration ... 141
10.6.5 Parameter ... 142
10.7 Netzwerkschnittstelle ... 143
10.7.1 Node Object ... 143
10.7.2 Bus Loop Monitor Objekt ... 145
10.7.3 Device Monitor Objekt ... 145
10.7.4 Twin Router Object ... 147
10.7.5 Channel Monitor Objekte ... 148
11 Schnittstellen ... 152
11.1 SNMP Interface ... 152
11.1.1 SNMP Funktionen ... 152
11.1.2 Konfiguration ... 152
11.1.3 Datenpunkte über SNMP ... 153
11.1.4 SNMP-Sicherheit ... 154
12 Netzwerkmedien ... 156
12.1 TP-1250 ... 156
12.2 FT-10 ... 156
12.3 RS-485 ... 157
12.4 Redundante Ethernet-Verkabelung ... 158
12.4.1 Verkabelungsoptionen ... 158
12.4.2 Upstream-Varianten ... 160
12.4.3 Voraussetzungen ... 161
12.4.4 Switch-Konfiguration ... 161
12.4.5 Verbindungstests ... 162
12.4.6 Beispielskonfiguration für Switches ... 163
12.5 WLAN ... 164
12.5.1 Einleitung ... 164
12.5.2 802.11s Mesh-Netzwerke ... 165
12.5.3 Hardware-Installation ... 166
13 L-IP Firmware Update ... 167
13.1 Firmware-Update über das Web-Interface ... 167
13.2 Firmware Update über IP ... 167
14 Fehleranalyse ... 169
14.1 LonMaker liefert eine Fehlermeldung beim Kommissionieren des L-IP ... 169
14.2 Paketweiterleitung schlägt fehlt wenn Channel-Timeout aktiv ist ... 170
14.3 Default Gateway Adresse ist falsch ... 170
14.4 TP-1250 Port funktioniert nicht ... 171
14.5 CEA-709 Activity LED blinkt rot ... 171

14.6 Die CEA-709 Activity LED und die Status LED blinken rot ... 171
14.7 IP-852 Datenverkehr kann am gesamten geswitchten IP Netzwerk gesehen werden ... 172
14.8 Technischer Support ... 172
14.9 Paketaufzeichnung ... 172
14.9.1 Konfiguration der Remote-Paketaufzeichnung ... 172
14.9.2 Aktivieren einer lokalen Aufzeichnung ... 173
14.9.3 Wireshark Remote-Aufzeichnung ... 174
15 Anwendungshinweise ... 178
16 Security-Leitfaden ... 179
16.1 Installationshinweise ... 179
16.2 Firmware ... 179
16.3 Ports ... 180
16.4 Dienste ... 180
16.5 Upgrade auf stärkere Schlüssel ... 181
16.6 Protokoll und Audit ... 182
16.7 Netzwerkzugriff ... 182
16.8 Passwortschutz ... 182
16.9 Verschlüsselung im Speicher ... 182
16.10 Sichere Entsorgung und Außerbetriebnahme ... 183
16.11 Informationsrichtlinie ... 183
17 Spezifikationen ... 184
17.1 Technische Spezifikationen ... 184
17.1.1 LIP-xxECRB ... 184
17.1.2 LIP-3ECTC, LIP-33ECTC, LIP-13ECTC ... 184
17.1.3 LIP-3333ECTC ... 185
17.2 FCC Hinweis ... 185
17.3 CE Hinweis ... 185
18 Quellenangabe ... 186
19 Versionsverzeichnis ... 187

Abkürzungen

10BaseT	10 Mbps Ethernet Netzwerk mit RJ-45 Stecker
Aggregation	Einpacken mehrerer CEA-709 Pakete in ein CEA-852 Paket
BOOTP	Bootstrap Protocol, RFC 1497
CC	Configuration Client, auch CN/IP-Gerät genannt
CN	Control Network
CN/IP	Control Network over IP
CN/IP Channel	logischer IP-Kanal, der CEA-709 Pakete nach dem CEA-852 Standard tunnelt
CN/IP packet	IP Paket, das ein oder mehrere CEA-709 Pakete enthält
CR	Channel Routing
CS	Konfigurationsserver der CEA-852 IP Geräte verwaltet
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DNS	Domain Name Server, RFC 1034
CEA-709	Protokollstandard für Feldbus-Netzwerke
CEA-852	Protokollstandard zum Tunneln von CEA-709 Paketen über IP Kanäle
IP	Internet Protocol
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LSD-Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, RFC 1321
NAT	Network Address Translation, RFC 1631
OPC	Open Process Control
SL	Send List
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
VNC	Virtual Network Computing
VNI	Virtuelles Netzwerk-Interface
VPN	Virtual Private Network
WLAN	Wireless LAN

1 Einleitung

1.1 Übersicht

1.1.1 L-IP

Der L-IP ist eine leistungsfähige, zuverlässige und sichere Netzwerkinfrastrukturkomponente, um CEA-709 Netzwerke über Intranet und das Internet zu verbinden. Er kann eingesetzt werden, um Filialen einer Handelskette zu vernetzen, um einen Hochgeschwindigkeits-Backbone-Kanal aufzubauen, oder als Netzwerkinterface für LNS basierende Netzwerkmanagementwerkzeuge zu dienen. Der eingebaute Konfigurationsserver kann bis zu 256 Geräte auf dem IP Kanal verwalten und ersetzt somit einen PC, der bisher als Konfigurationsserver dienen musste. Der L-IP kann hinter NAT-Routern und Firewalls eingesetzt werden und fügt sich somit nahtlos in bestehende Intranet Netzwerke ein. Er unterstützt DHCP in Intranet Netzwerken, auch wenn sich die IP Adresse ändert. Einfach zu verstehende Diagnose LEDs ermöglichen dem Systemintegrator dieses Gerät auf einfache Weise und ohne spezielles Expertenwissen zu installieren und im Fehlerfall entsprechend eine Fehlerbehebung durchzuführen. Der L-IP kann als Standard CEA-709 konfigurierter Router oder als selbstlernender Plug&Play Router („Smart Switch Modus“), basierend auf dem hocheffizienten, vielfach bewährten Routing-Core unserer Multiport-Plug&Play-L-Switch-Produkte, eingesetzt werden. Der selbstlernende Router benötigt kein Netzwerkmanagementwerkzeug zu seiner Konfiguration, sondern ist ein echtes Plug&Play-Gerät und somit eine einfach zu verwendende IP-Netzwerkinfrastrukturkomponente. Die integrierten, fortschrittlichen Netzwerkstatistik- und Diagnosefunktionen ermöglichen eine einfache Installation und einen zuverlässigen Betrieb des Netzwerkes über die gesamte Lebensdauer der Anlage. Die automatische Keep-Alive Funktionalität erhält IP Verbindungen aufrecht, auch in Zeiten wo normalerweise kein IP Verkehr zu erwarten ist und somit z.B. bei DSL Modems die Verbindung abgebaut werden würde. Die Multiportvariante des L-IP vereint die Funktionalität von zwei herkömmlichen L-IPs in einem Gerät. Dieser L-IP ist mit einem 100-BaseT Ethernet Port (CEA-852) und zwei FT-10 Ports (CEA-709) ausgestattet.

Der L-IP harmoniert perfekt mit unseren L-Switch Multi-Port Router, um gemeinsam eine hoch zuverlässige, komplett verwaltbare, Hochgeschwindigkeits-Netzwerkinfrastruktur für CEA-709 Netzwerke zu bilden. Die smarte Routing-Software detektiert die Bitrate am Kanal, lernt die Topologie des Netzwerkes (Domains, Subnet/Node Adressen, Gruppenadressen) und leitet die Pakete zwischen den Ports weiter. Die Verwendung von L-IP und L-Switch Geräten in einem Netzwerk mit strukturierter Verkabelung ist der Garant für die kostengünstigste Möglichkeit, Performanceprobleme im Netzwerk zu vermeiden.

Der L-IP sammelt laufend Statistikinformationen aus dem angeschlossenen Netzwerk (Kanallast, CRC Fehlerstatistik, Routingstatistiken, u.s.w.). Die L-IP Firmware verwendet diese wichtigen Betriebsparameter, um existierende oder sich anbahnende Probleme wie Überlastsituationen und Verbindungsprobleme frühzeitig dem Benutzer über einfach zu interpretierende Diagnose-LEDs anzuzeigen (siehe Abschnitt 6.4.10). Dieses sehr intuitive Benutzerinterface erlaubt selbst dem weniger geübten Installateur, einen problemlosen

Betrieb des Netzwerkes ohne zusätzliche Analysewerkzeuge und spezielles Fachwissen. Mit dem LSD Tool von LOYTEC können weitere wichtige Betriebsparameter des Netzwerkes dargestellt und ausgewertet werden. Kapitel 15 enthält mehr Informationen zum LSD Tool für Sie bereit.

Der eingebaute Web-Server ermöglicht die Konfiguration des L-IP mit einem einfachen Web-Browser wie z.B. Internet Explorer oder Netscape. Mittels Web Interface können auch die Konfigurationsdaten des Konfigurationsservers gesichert und wiederhergestellt werden und Statistikinformationen während des Betriebs sowie bei der Installation abgerufen werden.

Beginnend mit Firmwareversion 2.0 unterstützt der L-IP die Remote-LPA Funktionalität. Der Remote-LPA ist ein hervorragendes Analysewerkzeug zur Fehlersuche auf dem lokalen FT-10 oder TP-1250 Kanal, ohne dass der Protokollanalysator physikalisch an diesen Kanal angeschlossen wird. Die CEA-709 Datenpakete werden über den IP-852 Kanal an den Protokollanalysator geschickt, der sich irgendwo am IP-852 Kanal befinden kann. Bitte konsultieren Sie unsere Produktbeschreibung zum LPA-IP, um nähere Informationen zu diesem leistungsfähigen Analysewerkzeug zu erhalten. Der LPA-IP ist ein Muss für alle Systemintegratoren, die mit IP-852 Kanälen arbeiten.

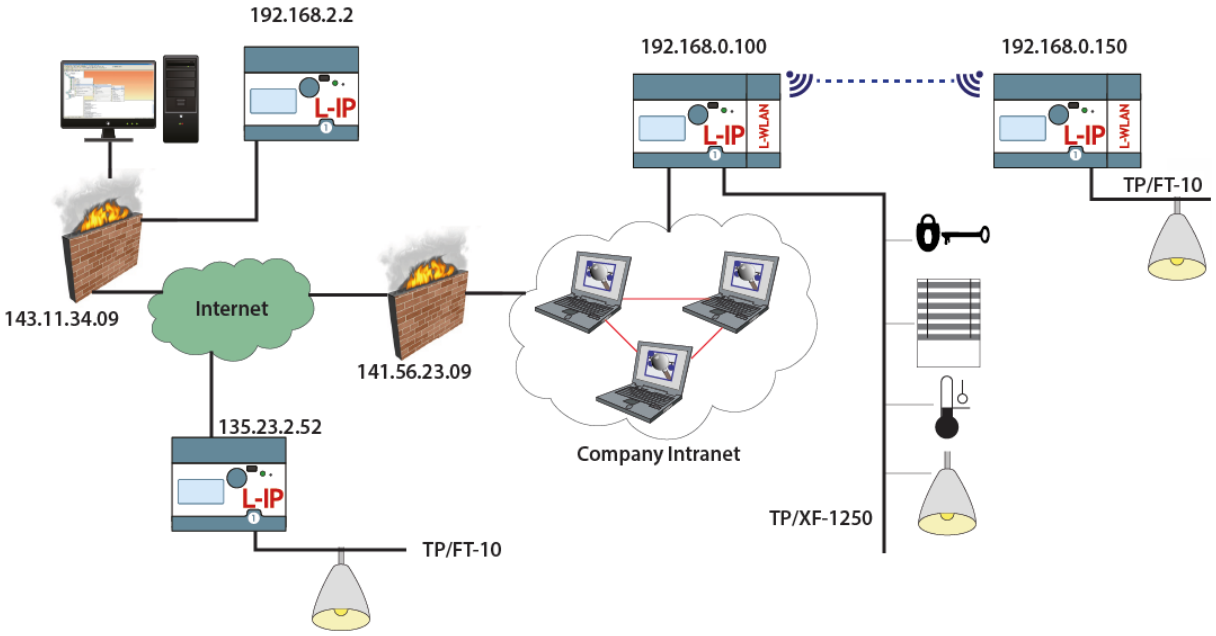


Abbildung 1: L-IP Anwendungsgebiet hinter einem NAT-Router oder direct and Internet angeschlossen

Die L-IP Modellserie C besitzt zwei Ethernet-Ports sowie eine LCD-Anzeige, mit der das Gerät einfach in Betrieb genommen werden kann. Auch die Wireshark Paketaufzeichnung ist auf diesen Geräten verfügbar.

Zusätzlich sind die L-IP Modelle der C-Serie auch mit einer integrierten Firewall und einem sicheren Web-Interface ausgestattet, das HTTPS und selbstsignierte oder CA-Zertifikate verwenden kann. Durch die Konfiguration von separaten IP-Netzwerken auf den beiden Ethernet-Anschlüssen kann das CEA-852-Netzwerk vollständig von der Konfiguration isoliert werden. Mit OpenVPN wird zusätzlich auch eine sichere Methode zur Fernwartung ermöglicht.

Zur perfekten Integration in Gebäude-Management Software wie dem LWEB-900 bieten die L-IP Modelle der C-Serie einen eingebauten OPC UA-Server mit Zertifikaten, der wichtige Betriebsparameter verfügbar macht. Zum verbesserten Verwalten in IT-Abteilungen bieten diese Modelle einen eigenen SNMP-Server. Gemeinsam mit dem LWLAN-800 Adapter

können diese Modelle sogar CEA-852 über ein WLAN betreiben. Damit können über einen Access Point am Ethernet-Netzwerk die FT-Kanäle über ein drahtloses Netzwerk verteilt werden.

Der L-IP kann in folgenden Anwendungsgebieten eingesetzt werden:

- Transportieren von CEA-709 Paketen über IP Kanäle (Intranet/Internet)
- CEA-709 Netzwerke über das Internet sicher verbinden
- Aufbau von Hochgeschwindigkeits-Backbone-Kanälen mit existierender IP-Infrastruktur
- Vernetzen von Liegenschaften und Filialen
- Konfigurationsserver für IP-basierte CEA-709 Geräte
- Netzwerk-Interface für LNS-basierte Netzwerkmanagementwerkzeuge (z. B. LonMaker, NL-220)
- Isolierung des lokalen Datenverkehrs vom Backbone-Verkehr
- Strukturierung von Netzwerken
- Erhöhung der physikalischen Ausdehnung und/oder Knotenanzahl eines Übertragungskanals,
- Verbindung von Kanälen mit unterschiedlichen Übertragungsmedien
- Netzwerküberwachung und Netzwerkmanagement
- Remote-LPA Funktion
- Verbinden von CEA-709 Netzwerken hinter NAT-Routern
- Verbinden von CEA-709 Netzwerken über ein WLAN

1.1.2 L-IP Redundant

Der L-IP Redundant CEA-709/IP Router stellt eine hervorragende Lösung für Netzwerke dar, in denen hohe Anforderungen an die Zuverlässigkeit der Kommunikation gestellt werden. Basierend auf der L-IP Plattform wurde er um Funktionen zum Aufbau einer redundanten Netzwerkinfrastruktur erweitert.

Als einzelnes Gerät kann der L-IP Redundant CEA-709/IP Router zur redundanten Ausführung von CEA-709 (TP/FT-10) Kanälen durch Bilden einer Ringtopologie eingesetzt werden. Durch den parallelen Einsatz von 2 Geräten kann auch der IP-Kanal redundant ausgeführt werden. In diesem Anwendungsfall wird die Zuverlässigkeit auch durch die gegenseitige Überwachung der beiden Geräte erhöht.

Zusätzlich kann der L-IP Redundant CEA-709/IP Router Knoten auf dem TP/FT-10 Kanal überwachen und einen Alarm absetzen, wenn ein Knoten ausfällt. Auf diesem Weg kann auch die Position eines Kabelbruchs erkannt werden. Der L-IP Redundant unterstütz lediglich den „Configured Router“ Modus.

So wie ein L-IP Router tunnelt auch ein L-IP Redundant CEA-709/IP Router CEA-709 Pakete über IP basierende Netzwerke (LAN, Intranet oder Internet). Der Router ist mit dem IP Netzwerk über einen Ethernetkanal verbunden. Die IP Konfiguration kann über DHCP bezogen oder manuell (Serielles Interface oder Web Interface) konfiguriert werden. Der

Benutzer muss lediglich die IP Adresse des CEA-852 Konfigurationsservers einstellen. Wird das Gerät hinter einem Router mit network address translation (NAT oder masquerading) betrieben, so unterstützt der L-IP Redundant CEA-709/IP Router Auto-NAT um auch mit dynamischen öffentlichen IP Adressen zu arbeiten. Die Konfiguration des eingebauten Configuration Servers kann über das Web Interface erstellt und in eine Datei gesichert werden. Die Konfiguration wird im Permanentspeicher gesichert, wodurch das Gerät eigenständig betrieben werden kann. Nach der Installation kann der L-IP Redundant CEA-709/IP Router Pakete zwischen dem IP Netzwerk und dem TP/FT-10 Kanal (Ringtopologie) routen. Daher können alle CEA-709 Netzwerke, die mit L-IP Routern verbunden sind, Daten über den CEA-852 Kanal austauschen. Erfolg die Anbindung der L-IP Router über unsichere IP Verbindungen wie dem Internet, so können alle CEA-852 Kanäle mit Hufe von Zeitstempel und MD5 Checksummen authentifiziert werden. Neben der eigentlichen Routingfunktionalität ist der L-IP Router ein leistungsfähiges Diagnosewerkzeug. Die einfach zu bedienende Benutzerschnittstelle ermöglicht einen raschen Überblick über den Zustand des Netzwerks. Sowohl der CEA-852 als auch der CEA-709 Kanal können mit Status-LEDs überwacht werden. Zur Fehlerdiagnose unterstützt der L-IP die remote LPA (LOYTEC Protocol Analyzer) Funktionalität, so dass das Netzwerk über das Internet analysiert werden kann. Mit dem L-IP Redundant CEA-709/IP Router wird der Aufbau eines redundanten und gleichzeitig wartungsfreundlichem Netzwerks eine einfache Aufgabe.

Der L-IP Redundant kann verwendet werden um

- eine redundante CEA-709 Netzwerkstruktur aufzubauen
- einen TP/FT-10 Kanal (Ringtopologie) auf Kabelbruch zu überwachen
- die Kommunikation auf einem TP/FT-10 Kanal bei einfachem Kabelbruch aufrecht zu erhalten
- den Zustand von Knoten auf einem CEA-709 Netzwerk zu überwachen
- einen Kabelbruch zu lokalisieren
- volle Redundanz auf dem IP Kanal und dem CEA-709 Kanal durch zwei parallel eingesetzte L-IP Redundant CEA-709/IP Router zu erreichen
- zwei Router gegenseitig zu überwachen
- Nachrichten und Alarme über SNVTs und LONMARK-Alarming an die Gebäudeleittechnik zu melden.

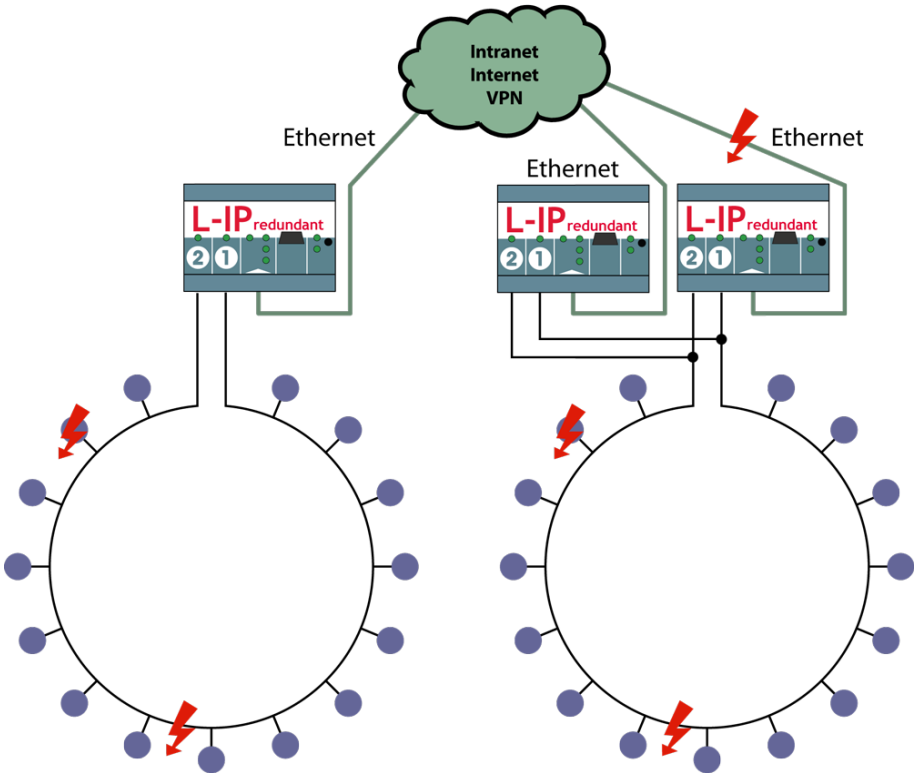


Abbildung 2: Verwendung des L-IP Redundant mit TP/FT-10 Kanälen in Ringstopologie sowie redundanter Routerstruktur

1.2 L-IP Modelle

Dieser Abschnitt bietet in Tabelle 1 eine Übersicht der unterschiedlichen L-IP Modelle. Die Tabelle hebt unterschiedliche Funktionen der einzelnen Modelle heraus. Modelle, die ein bestimmtes Feature unterstützen, sind mit einem Häkchen (✓) in der entsprechenden Spalte markiert. Wenn ein Feature in einem bestimmten Modell nicht verfügbar ist, ist die Spalte an dieser Stelle leer.

Modell / Features	LIP-33ECRB	LIP-1ECTC	LIP-3ECTC	LIP-13ECTC	LIP-33ECTC	LIP-333ECTC
CEA-709 Router	✓	✓	✓	✓	✓	✓
Redundant Router	✓					
CEA-709 Ports	2	1	1	2	2	4
Remote LPA	✓	✓	✓	✓	✓	✓
OPC XML-DA		✓	✓	✓	✓	✓
OPC UA		✓	✓	✓	✓	✓
SNMP		✓	✓	✓	✓	✓
LCD Display		✓	✓	✓	✓	✓
Serielle Konsole, DIP-Schalter	✓					
USB		✓	✓	✓	✓	✓
Ethernet Switch/Hub		✓	✓	✓	✓	✓
WLAN, LTE		✓[1]	✓[1]	✓[1]	✓[1]	✓[1]
SSH, HTTPS, Firewall, VPN		✓	✓	✓	✓	✓

[1] Zum Betrieb dieser Protokolle wird ein Erweiterungsmodul benötigt und muss separat bestellt. werden

Tabelle 1: Verfügbare Funktionen in den unterschiedlichen L-IP Modellen.

1.3 Umfang dieses Dokumentes

Dieses Dokument dient zur Beschreibung des L-IP Routers mit 8.6.0.

2 Haftungsausschluss Cyber-Sicherheit

LOYTEC bietet ein Portfolio von Produkten, Lösungen und Systemen mit Sicherheitsfunktionen, die den sicheren Betrieb von Geräten, Anlagen und Netzwerken im Bereich der Gebäudeautomation und Leittechnik ermöglichen. Damit Geräte, Anlagen, Systeme und Netzwerke stets vor Online-Bedrohungen geschützt sind, benötigt es ein ganzheitliches Sicherheitskonzept, das auf dem neuesten Stand der Technik implementiert und auf einem aktuellen Stand gehalten wird. Das Portfolio von LOYTEC ist dabei nur ein Bestandteil eines solchen Gesamtkonzeptes.

Der Kunde ist dafür verantwortlich, unbefugten Zugang zu den Geräten, Anlagen, Systemen und Netzwerken zu unterbinden. Diese sollten nur mit einem Netzwerk oder dem Internet verbunden werden, wenn angemessene Sicherheitsvorkehrungen vorhanden sind (z.B. Firewalls, separate Netzwerke) und eine Verbindung für den Betrieb erforderlich ist. Darüber hinaus sind die Empfehlungen von LOYTEC zur Absicherung von Geräten im Security-Leitfaden (Kapitel 16) zu befolgen. Für ergänzende Informationen kontaktieren Sie bitte Ihren Ansprechpartner bei LOYTEC oder besuchen Sie unsere Webseite.

LOYTEC arbeitet ständig an einer Weiterentwicklung der bestehenden Produkte um den letzten Sicherheitsstandards zu folgen. Daher empfiehlt LOYTEC dringend, Updates zu installieren, sobald diese zur Verfügung stehen, und stets die neusten Software-Versionen zu verwenden. LOYTEC weist ausdrücklich darauf hin, dass durch Verwendung älterer Versionen oder dem Unterlassen von Updates das Risiko für Online-Bedrohungen steigt, wodurch das Gerät bekannten und dokumentierten Sicherheitsbedrohungen ausgesetzt wird, was zu unbefugtem Zugriff auf das Gerät, zur Änderung oder Offenlegung von Konfigurations- und vertraulichen Benutzerdaten oder zu einer Unterbrechung des Gebäudeautomationsbetriebs führen kann. LOYTEC übernimmt keine Haftung für Sicherheitsvorfälle, Unfälle oder Ausfälle, die auf die Verwendung eines Produkts zurückzuführen sind, für das verfügbare Sicherheitsupdates nicht installiert wurden.

3 Sicherheitshinweise



VORSICHT

Allgemeine Sicherheitsvorschriften

Bitte beachten Sie die folgenden, allgemeinen Vorschriften bei der Projektierung und Ausführung:

- Maßnahmen bzw. Verbote zur Vermeidung der Gefahr Elektrizitäts- und Starkstromverordnungen des jeweiligen Landes.
- Andere einschlägige Vorschriften des jeweiligen Landes.
- Hausinstallationsvorschriften des jeweiligen Landes.
- Vorschriften des Energielieferanten.
- Allfällige Spezifikationen, Schemata, Dispositionen, Kabellisten und Anordnungen des Kunden oder des beauftragten Ingenieurbüros.
- Vorschriften Dritter (z.B. Generalunternehmer oder Bauherr).



VORSICHT

Länderspezifische Sicherheitsvorschriften

Die Nichtbeachtung von länderspezifischen Sicherheitsvorschriften kann zu Sach- und Personenschäden führen. Daher halten Sie die länderspezifischen Bestimmungen und die entsprechenden Sicherheitsrichtlinien ein.



VORSICHT

Elektrische Sicherheit

Im Wesentlichen beruht Die elektrische Sicherheit bei Gebäudeautomationssystemen von LOYTEC auf der Verwendung von Kleinspannung mit sicherer Trennung gegenüber Netzspannung.



VORSICHT

IEC (SELV, PELV) (weltweit)

Es ergibt sich in Abhängigkeit von der Kleinspannungserdung (⊥ AC 24V) eine Anwendung nach SELV oder PELV gemäß der IEC 60364-4-41 Errichten von Niederspannungsanlagen:

- Ungeerdet = Sicherheitskleinspannung SELV (Safety Extra Low Voltage).
- Geerdet = Schutzkleinspannung PELV (Protected Extra Low Voltage)



VORSICHT

NEC (Nordamerika)

Es müssen Class 2-Trafos mit Energiebegrenzung auf 100 VA oder Class 2-Kreise mit max. 100 VA (unter Verwendung eines nicht energie-begrenzenden Trafos von max. 400VA) kombiniert mit Überstrombe-grenzungen (T-4A-Sicherungen) für jedes einzelne 24VAC-Gerät verwendet werden. Es sind mehrere Sicherungen für mehrere isolierte Sekundärkreise pro Trafo möglich. Dasselbe gilt für Netzteile mit 24VDC.



VORSICHT

Gerätesicherheit

Die gerätetechnische Sicherheit wird u. a. durch Versorgung mit Kleinspannung 24 VAC bzw. 24 VDC und einer doppelten Isolation zwischen Netzspannung 230 VAC, 24 VAC Kreisen und dem Gehäuse gewährleistet oder durch Versorgung mittels Power over Ethernet (PoE Class 1). Außerdem sind die spezifischen Vorschriften für die elektrische Verdrahtung gemäß diesem Handbuch zu beachten.



VORSICHT

Installationspersonal

Elektrische Installationsarbeiten dürfen ausschliesslich von Fachpersonal ausgeführt werden.



VORSICHT

Einbau nach Schutzklasse II

Bei der Montage von LOYTEC Geräten, die nach Schutzklasse II designed wurden, sind folgende Anforderungen zu erfüllen:

- Der Schutz gegen elektrischen Schlag (Berührschutz) ist durch ein entsprechendes Gehäuse zu gewährleisten.
- Beim Einbau in Geräte der Schutzklasse II ist eine passende Zugentlastung der Anschlussdrähte vorzusehen.



VORSICHT

Einbauort

LOYTEC-Geräte sind für den Einbau in ein Gehäuse vorgesehen:

- Schaltschränke
- Verteilerboxen
- Einbau in Zwischendecken
- Leuchteneinbau



VORSICHT

Umgebungsbedingungen

LOYTEC-Geräte müssen in einer trockenen und sauberen Umgebung betrieben werden. Zusätzlich müssen die im jeweiligen Produktdatenblatt angegeben Betriebsbedingungen eingehalten werden.



VORSICHT

Erdung von ⊥ (Systemnull AC/DC 24V)

Bei der Erdung von Systemnull ⊥ 24VAC sind folgende Punkte zu beachten:

- Es ist grundsätzlich sowohl die Erdung als auch die Nicht-Erdung von Systemnull der Betriebsspannung 24VAC zulässig. Maßgebend sind die örtlichen Vorschriften und Gepflogenheiten. Eine Erdung kann aus funktionellen Gründen erforderlich oder unzulässig sein.
- Es wird empfohlen, 24VAC-Systeme zu erden, sofern dies nicht den Angaben des Herstellers widerspricht.
- Systeme mit PELV dürfen zur Vermeidung von Erdschlaufen nur an einer Stelle im System mit Erde verbunden werden. Wenn nicht anders angegeben, meistens beim Trafo.
- Dasselbe gilt für Netzteile mit 24VDC.



VORSICHT

Funktionserde ⏚

Der Anschluss der Funktionserde muss installationsseitig mit dem Gebäude-Erdungssystem (PE) verbunden werden.



VORSICHT

Betriebsspannung 24V AC/DC

Die Versorgung muss den Anforderungen für SELV oder PELV genügen. Zulässige Abweichung der Nennspannung:

- Am Trafo bzw. Netzteil: 24V AC/DC -10 … + 10%
- Am Gerät: 24V AC oder DC ±10 %



VORSICHT

Spezifikation für 24VAC-Trafos

IEC: Sicherheitstrafos gem. IEC 61558 mit doppelter Isolation, ausgelegt für 100% Einschaltdauer zur Versorgung von SELV oder PELV-Stromkreisen.

USA: Class 2-Kreise gem. UL 5085-3.

Aus Effizienzgründen (Wirkungsgrad) sollte die dem Trafo entnommene Leistung mindestens 50% der Nennlast betragen.

Die Nennleistung des Trafos muss mind. 25 VA betragen. Bei einem kleiner dimensionierten Trafo wird das Verhältnis von Leerlaufspannung zur Spannung bei Volllast ungünstig (> + 20%).



VORSICHT

Spezifikation für 24VDC-Netzteile

Netzteile müssen für 100% Einschaltdauer zur Versorgung von SELV- oder PELV-Stromkreisen ausgelegt sein.

USA: Class 2-Kreise gem. UL 5085-3.

Aus Effizienzgründen (Wirkungsgrad) sollte die dem Netzteil entnommene Leistung mindestens 50% der Nennlast betragen.



VORSICHT

Absicherung der Betriebsspannung 24VAC

Trafos müssen sekundärseitig abgesichert werden, dies gemäß Trafodimensionierung und entsprechend der effektiven Belastung aller angeschlossenen Geräte:

Den 24 VAC Leiter (Systempotential) immer absichern,

zusätzlich den Leiter ⊥ (Systemnull) absichern, wo vorgeschrieben.



VORSICHT

Absicherung der Betriebsspannung 24VDC

24V-Netzteile müssen kurzschlussfest sein oder eine interne Feinsicherung besitzen.

Lokale Vorschriften sind zu beachten.



VORSICHT

Absicherung der Netzspannung

Trafos/24VDC-Netzteile müssen primärseitig mittels Schaltschrank-sicherung (Steuersicherung) abgesichert werden.



VORSICHT

Power over Ethernet (PoE)

LPAD-7 Touch Panels benötigen eine Versorgung gem. PoE Class 1 (max. 12W), die konform zu IEEE 802.3at-2009 sein muss.

Für die Versorgung der PoE-Switches beachten Sie bitte die Vorschriften der Hersteller.



VORSICHT

Geräteeinbau/ausbau nur im Spannungsfreiem Zustand

Stellen Sie sicher, daß die Stromversorgung ausgeschaltet ist bevor sie mit der Installation oder Deinstallation von LOYTEC-Geräten beginnen. Schliessen Sie die Geräte NICHT bei eingeschalteter Stromversorgung an oder ab, solange keine anderslautende Anweisung haben. Montieren oder Demontieren Sie Geräte NICHT bei eingeschalteter Stromversorgune, es sei denn Sie haben andere Anweisungen erhalten.



VORSICHT

Absicherung der Versorgung

Bei der Installation von LOYTEC-Geräten ist der Versorungskreis mit einer entsprechend bemessenen Sicherung oder einem thermischen Schutzschalter abzusichern.



VORSICHT

Versorgungspannung

Schliessen Sie keine Spannung an die Versorgungsklemmen an, welche den spezifizierten Maximalwert übersteigt. Beachten Sie die Spannungsangaben auf dem Produktetikett und/oder im Datenblatt.



VORSICHT

DALI ist FELV (Funktionskleinspannung)

Eine DALI-Linie ist als Funktionskleinspannung zu behandeln. Da sie nicht SELV (Sicherheitskleinspannung) ist, sind die Installationsrichtlinien für Niederspannung anzuwenden.



VORSICHT

DALI Verdrahtung

Eine DALI-Linie darf im selben Kabel oder als Einzelleiter im selben Kabelkanal wie Netzspannung installiert werden. Die DALI-Linie darf eine maximale Länge von 300m bei einem Leiterquerschnitt von 1.5mm^2 (AWG15) aufweisen oder es muss sichergestellt sein, dassder Spannungsabfall an der DALI-Linie 2V nicht überschreitet.



VORSICHT

Achtung auf Fremdspannungen

Jedes irgendwie geartetes Einschleusen oder Verschleppen von gefährlichen Spannungen auf die Kleinspannungskreise des Systems (z.B. durch falsche Verdrahtung) ist unbedingt zu vermeiden und stellt eine unmittelbare Gefahr für Personen dar bzw. kann zur gänzlichen oder teilweisen Zerstörung des Gebäudeautomationssystems führen.

4 Was ist neu im L-IP

4.1 Neuigkeiten im L-IP 8.6.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Zero-Config-IP

Die Standardeinstellung der Ethernet-Schnittstelle bezieht IP-Adressen über DHCP. Ist kein DHCP-Server vorhanden oder vorübergehend nicht erreichbar, weist die neue Zero-Config-IP-Funktion eine IP-Adresse aus dem Bereich der automatischen privaten IP-Adressierung (APIPA) 169.254.0.1 bis 169.254.255.254 zu. Einmal zugewiesen, bleibt diese Auto-IP-Adresse auch über Neustarts hinweg erhalten. Geräte mit Auto-IP können über ihren mDNS-Namen (d. h. hostname.local) gefunden werden.

LDAP-Benutzerauthentifizierung

Die Gerätefirmware unterstützt die LDAP-Integration zur Benutzerauthentifizierung. LDAP-Benutzer ergänzen die integrierten und lokal definierten Benutzer. Die LDAP-Konfiguration legt den LDAP-Server, den Bind-Benutzer/Passwort sowie die Benutzer- und Gruppenabfragen fest. Lokale Benutzerrollen werden bestimmten LDAP-Gruppen zugeordnet. Secure LDAP wird ebenfalls unterstützt. Die Web-Oberfläche zur LDAP-Konfiguration ist in Abbildung 3 dargestellt.

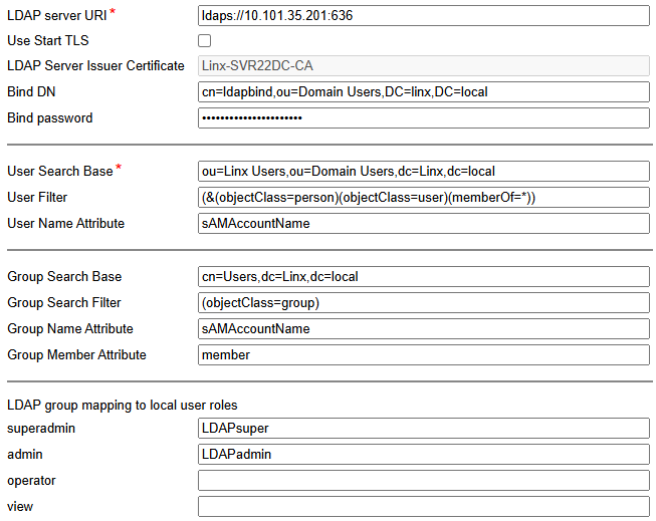


Abbildung 3: Web-Oberfläche zur LDAP-Konfiguration.

VNC-Verbindung über die Web-Oberfläche

Das LCD-Display von LOYTEC-Geräten kann über das Netzwerk per VNC-Verbindung bedient werden. Das VNC-Protokoll steht nun auch über eine Websocket-URI auf dem Gerät

für sogenannte ‚noVNC'-Clients zur Verfügung. Dies ist eine sichere Alternative zum bisherigen VNC-Port. Die Web-UI des Geräts bietet eine einfache VNC-Connect-Schaltfläche, um den Inhalt des LCD-Displays über diesen sicheren Websocket-Kanal in der Web-UI zu öffnen. Ein Beispiel ist in Abbildung 4 dargestellt.

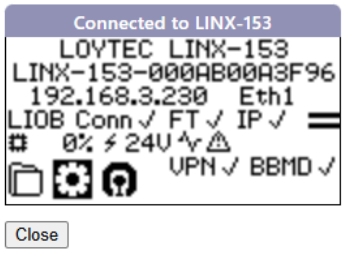


Abbildung 4: Secure noVNC Popup-Fenster auf der Web-Oberfläche.

4.2 Neuigkeiten im L-IP 8.4.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Erhöhte Sicherheit für Benutzerkonten und View-Rolle

Die integrierten Benutzerkonten (Admin, Operator, Guest) können deaktiviert werden, um Angriffe auf diese bekannten Konten zu verhindern. Das Admin-Konto kann nur deaktiviert werden, wenn stattdessen ein benutzerdefiniertes Konto mit der Superadmin-Rolle erstellt wurde. Für alle Konten werden in der Standardeinstellung sichere Passwörter erzwungen.

Die neue Rolle „View" ermöglicht es diesen Benutzern, nur Konfigurationseinstellungen anzuzeigen. Ein View-Benutzer kann keine Konfigurationseinstellungen ändern.

Gerätesuche über loytec.local

Nicht konfigurierte LOYTEC-Geräte ab Firmware 8.4.0 können nun auch ohne Kenntnis der IP-Adresse über die Webseite „loytec.local" gefunden werden. Die Suche wird eine mDNS-Erkennung im lokalen Netzwerk implementiert. Es wird eine Gerätesuchseite mit Links zu allen gefundenen Geräten angezeigt.

Konfiguration einer Internet-Failover-Schnittstelle

LOYTEC-Geräte unterstützen mehrere Pfade zum Internet. Beispielsweise Ethernet und eine angeschlossene LTE-800-Schnittstelle. Für solche Szenarien kann eine Failover-Schnittstelle ausgewählt werden. Diese dient als Standardroute zum Internet, falls die primäre Schnittstelle die Internetverbindung verliert. Die Konfiguration erfolgt auf der Registerkarte „IP-Host".

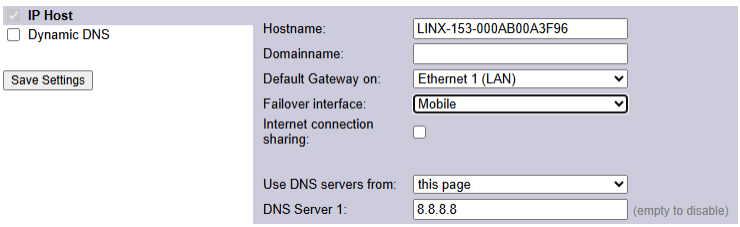


Abbildung 5: Konfiguration einer Internet-Failover-Schnittstelle.

4.3 Neuigkeiten im L-IP 8.2.8

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Unterstützung für neues Modell LIP-13ECTC

Der LIP-13ECTC ist ein Multiport-L-IP-Router mit einem TP-1250-Port, einem FT-10-Port und einem IP-852-Kanal.

Neuer L-Switch-Modus

Ein neuer Gerätebetriebsmodus wurde hinzugefügt: Der L-Switch-Modus. Dieser Modus ist für Multiport-L-IP-Modelle verfügbar (d.h. mit mehr als einem CEA-709-Port). Im L-Switch-Modus ist die IP-852-Schnittstelle deaktiviert und das Gerät verhält sich wie ein L-Switch zwischen den CEA-709-Ports. In diesem Modus ist der L-IP vollständig Plug-and-Play und kann auf dem LCD-Display eingerichtet werden. Es ist keine weitere Konfiguration auf der Weboberfläche erforderlich. Das macht den L-IP zu einem idealen Drop-in-Ersatz für gängige LON-Router von Drittanbietern.

4.4 Neuigkeiten im L-IP 8.2.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Unterstützung für neue A64-Modelle

Ab sofort werden die neuen L-IP-Modelle auf Basis der A64-Hardware unterstützt. Die neue Firmware enthält außerdem ein umfangreiches Sicherheitsupgrade auf OpenSSL 3.1.

4.5 Neuigkeiten im L-IP 8.0.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Neue WLAN Konfigurations-Reiter

Die WLAN-Konfiguration der Portkonfiguration wurde neu überarbeitet, um den Anwendungsfällen von Client und Access Point (AP) besser gerecht zu werden. Die Registerkarten heißen jetzt **WLAN Client** und **WLAN Access Point**. Diese Registerkarten sind auf jene Einstellungen beschränkt, die für ihre jeweilige Verwendung nötig sind.

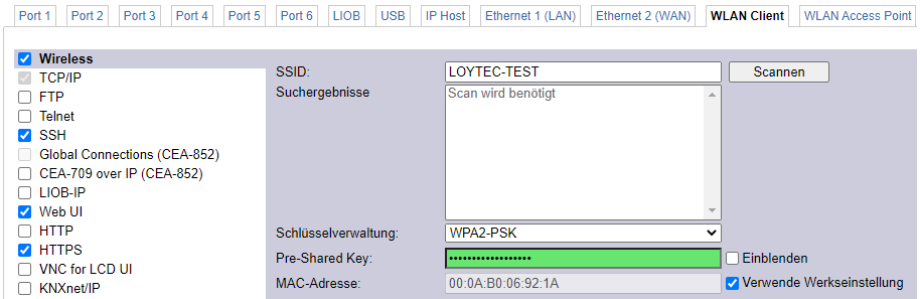


Abbildung 6: Neue WLAN-Konfiguration

4.6 Neuigkeiten im L-IP 7.6.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

WiFi Enterprise

Um die Sicherheit in einem WiFi-Netzwerk weiter zu erhöhen, unterstützen IT-Abteilungen die 802.1X-Authentifizierungsmethode für WiFi, auch bekannt als WiFi Enterprise. LOYTEC-Geräte können WiFi Enterprise in den Wireless-Einstellungen aktivieren, indem sie bei der Schlüsselverwaltung WPA2-ENTERPRISE auswählen. Unterstützt werden die Authentifizierungsverfahren Protected EAP (PEAP), Tunneled TLS (TTLS) und EAP-TLS (über Zertifikate).

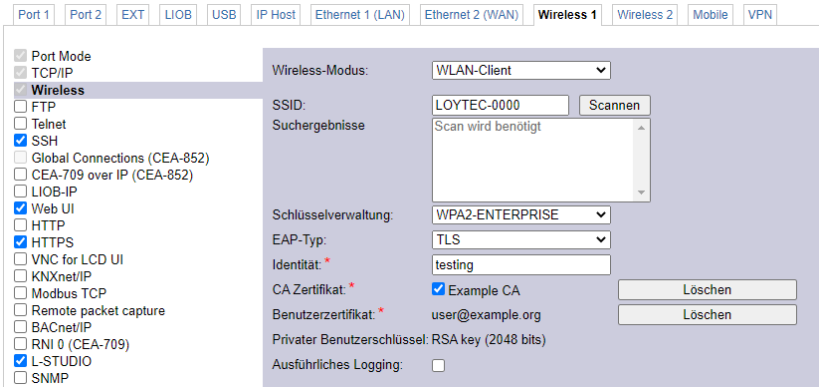


Abbildung 7: Konfiguration für WiFi Enterprise.

4.7 Neuigkeiten im L-IP 7.4.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Neue Menüstruktur am Web-Interface

Die Menüstruktur auf der Web-Benutzeroberfläche wurde so gestaltet, dass sie intuitiver und nach häufigen Aktionen gruppiert ist. Neue Einträge der obersten Ebene helfen dabei, die Menüs in typische Aufgabenbereiche wie Statistiken, Datenanzeige, Inbetriebnahme, Konfiguration, Programmierung, Sicherheit und Wartung zu organisieren.

Benutzerverwaltung am Gerät

LOYTEC-Geräte bieten jetzt eine einfache Benutzerverwaltung zum Erstellen von Benutzern und Kennwörtern vor Ort. Den Benutzern können Rollen zugewiesen werden, z.B. für „admin“, „operator“ oder „lweb“. Benutzer mit der Rolle „lweb“ dürfen nur LWEB-802/803-Visualisierungsprojekte verwenden und haben keine anderen Befugnisse für den Betrieb des Geräts.

Die Web-Benutzeroberfläche auf dem Gerät ermöglicht das Erstellen, Löschen und Ändern von Benutzern sowie das Zuweisen von Rollen. Beispielsweise kann ein zusätzlicher Administrator erstellt werden, der das Gerät konfigurieren darf, ohne das Haupt-administratorkennwort zu kennen. Dieses Benutzerkonto kann einfach wieder deaktiviert werden.

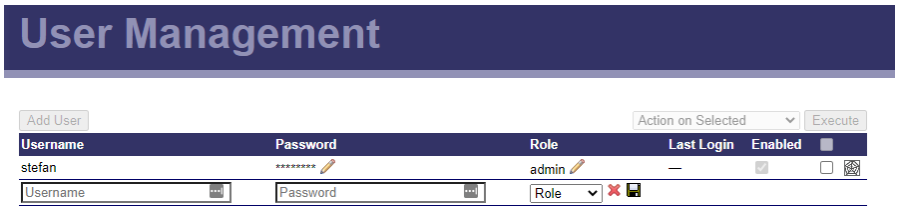


Abbildung 8: Benutzerverwaltung am Gerät

Authentifizierung an einem Netzwerkanschluss

Um die Sicherheit bei der Netzwerkinstallation weiter zu erhöhen, unterstützen IT-Abteilungen die 802.1X-Portauthentifizierungsmethode. Nach diesem Standard muss ein Gerät seinen Port am Netzwerk-Switch authentifizieren, bevor Datenverkehr in das Netzwerk zugelassen wird.

LOYTEC-Geräte können die 802.1X-Portauthentifizierung in den Portmoduseinstellungen aktivieren. Die Authentifizierungsmethoden Protected EAP (PEAP), Tunneled TLS (TTLS) und EAP-TLS (unter Verwendung von Zertifikaten) werden unterstützt.

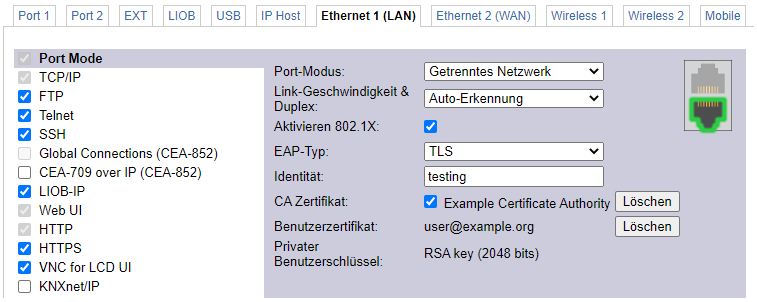


Abbildung 9: Konfiguration der 802.1X-Portauthentifizierung.

4.8 Neuigkeiten im L-IP 7.2.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Unterstützung für LTE

LOYTEC-Geräte unterstützen jetzt die LTE-800- Mobilfunkschnittstelle. Diese Schnittstelle wird über den USB-Anschluss angeschlossen und bietet Zugang zum LTE-/UMTS-/GSM-Mobilfunknetz. Es muss lediglich eine SIM-Karte Ihres Providers eingelegt werden und das LOYTEC-Gerät ist im Mobilfunknetz betriebsbereit. Der Portkonfiguration wurde eine Registerkarte **Mobile** hinzugefügt, welche die Konfiguration des LTE-800 erlaubt. Aktivieren Sie einfach das Mobilfunknetz, geben Sie Ihre APN-Daten ein und wählen Sie aus, welche Protokolle auf LTE aktiviert werden sollen.

Der VPN-Client kann auch im LTE-Mobilfunknetz verwendet werden.

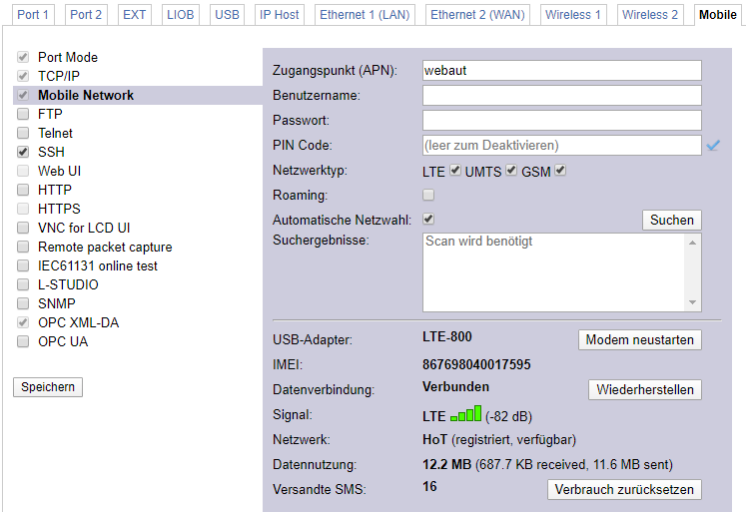


Abbildung 10: LTE-800 Mobilfunk-Konfiguration.

Internet-Verbindung gemeinsam nutzen

In Kombination mit einer LTE-800-Mobilfunkschnittstelle kann ein LOYTEC-Gerät als NAT-Router fungieren, um die mobile Internetverbindung mit anderen Geräten im LAN zu teilen. Zu diesem Zweck kann die Funktion **Internetverbindung gemeinsamen nutzen** auf der Registerkarte **IP-Host** aktiviert werden, wo das Standard-Gateway zur Verbindung ins Internet ausgewählt wird. Andere Geräte im LAN müssen die IP-Adresse des LOYTEC-Geräts angeben, das die Verbindungsfreigabe als Standard-Gateway anbietet. Auf diese Weise können lokale Geräte NTP, VPN-Client oder andere Internetdienste verwenden.

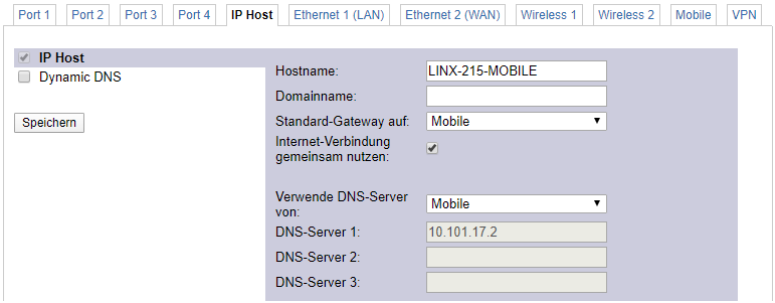


Abbildung 11: Internet-Verbindung gemeinsam nutzen

Dynamic DNS

LOYTEC-Geräte können jetzt einen Dynamic DNS-Dienst verwenden, um einen öffentlichen DNS-Namen zu registrieren. Dadurch ist das Gerät über eine öffentliche IP-Adresse erreichbar, die sich auch im Laufe der Zeit ändern kann, z.B. über eine mobile LTE-800-Mobilfunkschnittstelle, die eine IP-Adresse vom Mobilfunkanbieter zugewiesen bekommt. Eine Reihe Dynamic DNS-Anbieter ist vorkonfiguriert und kann auf der Registerkarte **IP-Host** der Portkonfiguration ausgewählt werden (siehe Abbildung 12).

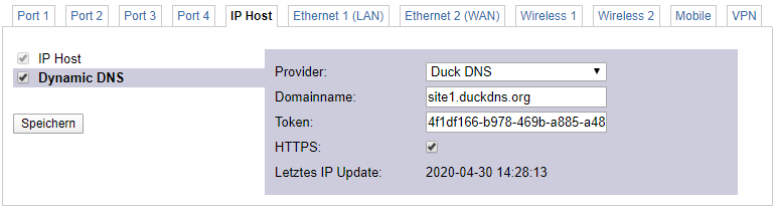


Abbildung 12: Dynamic DNS Einstellungen

Absicherung von Gebäudeautomationsprotokollen mittels VPN

Diese Firmware-Version verbessert die Flexibilität und Kontrolle darüber, welche Gebäudeautomationsprotokolle direkt über VPN verfügbar sind. Der Portkonfiguration wurde eine separate Registerkarte **VPN** hinzugefügt, über die IP-basierte Protokolle direkt auf dem VPN-Client gebunden werden können. Dies sichert effektiv einige ansonsten ungesicherte Protokolle wie CEA-852. Bei Verwendung auf der VPN-Schnittstelle wird den Protokollen eine VPN IP-Adresse zugewiesen, womit das LOYTEC-Gerät als Protokollknoten auch über Multi-NAT Zugangsnetze wie LTE erreichbar wird.

Richten Sie beispielsweise einfach den CEA-852-Konfigurationsserver auf der VPN-Schnittstelle ein und fügen Sie alle anderen CEA-852-Clients auf demselben VPN hinzu. Jeder Knoten richtet einen sicheren Kanal zum OpenVPN-Server-Hub ein, welcher dann den Verkehr zu den kommunizierenden Knoten weiterleitet. Dabei wird der Datenverkehr niemals unverschlüsselt übertragen.

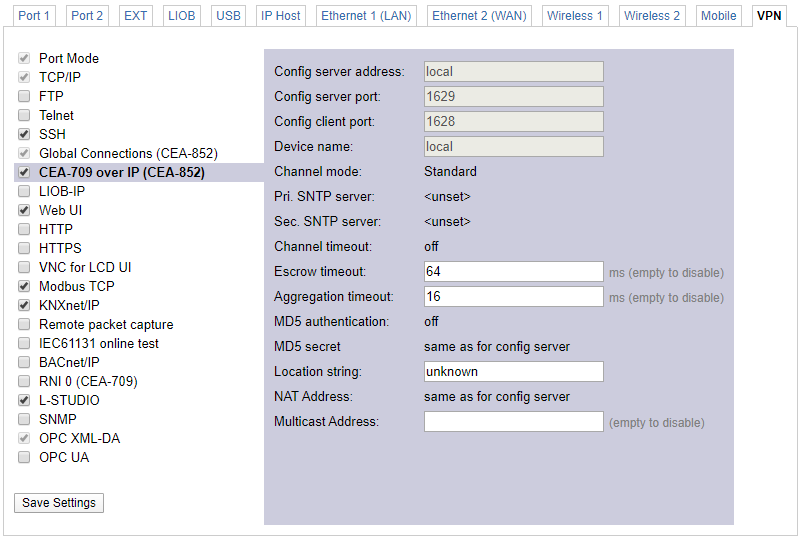


Abbildung 13: VPN Karteikarte auf der Seite zur Portkonfiguration.

4.9 Neuigkeiten im L-IP 7.0.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

VPN

LOYTEC-Geräte unterstützen die Einwahl in ein Virtuelles Privates Netzwerk (VPN). Diese neue Funktion setzt auf die weit verbreitete, offene Protokolltechnologie OpenVPN auf. Eine OpenVPN-Konfigurationsdatei (.ovpn) wird über das Web-Interface aufgespielt, die jene OpenVPN-Client-Konfiguration enthält, mit der sich das LOYTEC-Gerät in einen VPN Server einwählen kann. Jede herkömmliche OpenVPN-Konfiguration kann dazu verwendet werden, die Auto-Login unterstützt (d.h. kein Passwort beim Verbindungsaufbau benötigt). Nachdem sich das LOYTEC-Gerät im VPN registriert hat, ist es über seine VPN-Adresse erreichbar.

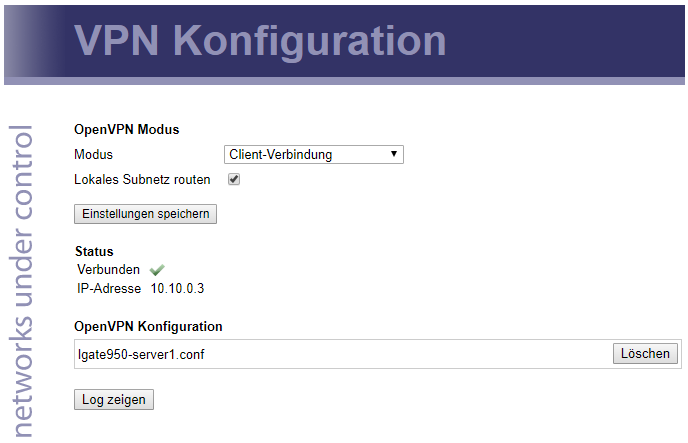


Abbildung 14: VPN Client-Konfiguration auf dem Web-Interface

Durch das Aufsetzen eines VPN-Clients am LOYTEC-Gerät können diverse Probleme über NAT-Router umgangen werden, weil keine Port-Weiterleitung konfiguriert werden muss. Das Gerät wählt sich nach außen bei dem OpenVPN-Server ein, der über seine IP-Adresse öffentlich erreichbar ist und etabliert einen VPN-Kanal. Dieser Kanal bietet eine sichere Verbindung für alle Gebäudeprotokolle, wie z.B. BACnet/IP, Modbus TCP oder CEA-852. Als Teil eines VPNs ist das LOYTEC-Gerät auch in Multi-NAT-Umgebungen von außen erreichbar, wie es beispielsweise über einen LTE-Zugang der Fall ist.

Als alternative Methode kann auf dem LOYTEC-Gerät ein „Simple Server“ Modus aktiviert werden. In diesem Modus agiert das Gerät selbst als OpenVPN Server und bietet den Download einer Client-Konfiguration vom Web-Interface an. Diese Datei kann auf einem beliebigen OpenVPN-Client installiert werden und ermöglicht die Verbindung zum LOYTEC-Gerät über den sicheren VPN-Kanal. Es kann immer nur ein Client gleichzeitig mit dem Gerät verbunden sein.

4.10 Neuigkeiten im L-IP 6.4.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Lokalisierung des Web-Interface

Das gesamte Web-Interface am Geräte wurde in den Sprachen Deutsch, Französisch und Chinesisch lokalisiert. Ändern Sie einfach die Sprache auf der LCD-Anzeige oder direkt am Web-Interface über das neue Flaggen-Symbol in der rechten oberen Ecke. Die Änderung wird sofort wirksam und benötigt keinen Neustart.

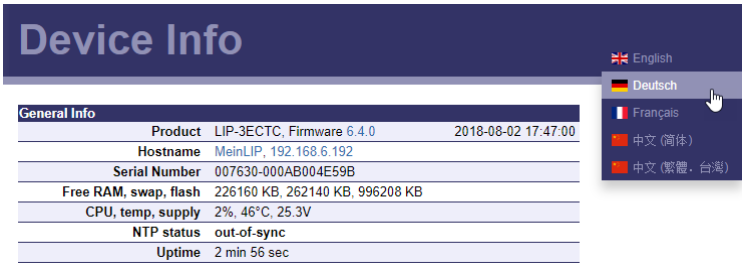


Abbildung 15: Sprachauswahl am Web-Interface

Sicherer Neustart und Auto-Login

Das Ändern der IP-Einstellungen und der darauffolgende Neustart konnten das Gerät unerreichbar Machen, wenn etwas anders als erwartet war. Die neue sichere Neustart-Funktion hilft in dieser Situation, indem die Einstellungen rückgängig gemacht werden, falls nicht innerhalb von 5 Minuten nach dem Neustart über das Web-Interface eingeloggt wird. Das selbst Aussperren durch eine Fehleinstellung in der IP-Adresse ist damit nicht mehr möglich.



Abbildung 16: Die sichere Neustart-Seite schlägt die neue IP-Adresse vor.

Eine weitere neue Funktion, die dabei hilft eingeloggt zu bleiben, ist das Session Auto-Login. Nachdem das Gerät neu gestartet hat, stellt das Web-Interface die vorige Sitzung wieder her und loggt sich automatisch wieder ein. Selbst bei Änderung der statischen IP-Adresse versucht das Gerät sich mit der neuen Adresse zu verbinden oder schlägt Links vor, über die die Info-Seite unter der neuen Adresse erreichbar sein wird.

Gerätesicherung vor dem Upgrade

Die Funktion zur Firmware-Aktualisierung wurde weiter verbessert, indem eine Gerätesicherung vor dem Upgrade erstellt wird. Diese Funktion wurde sowohl in die Geräte als auch in den Configurator eingebaut. Sie ist optional und kann bei Bedarf auch durch eine Check-Box deaktiviert werden.

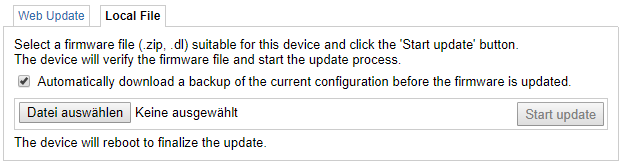


Abbildung 17: Gerätesicherung vor dem Upgrade am Web-Interface.

LCD Anzeige

Die Benutzerführung auf der LCD-Anzeige wurde lokalisiert und unterstützt nun auch die chinesische Sprache (vereinfacht und traditionell). Die Spracheinstellung kann direkt auf der Hauptseite angewählt werden und wird sofort und ohne Neustart aktiv.

Die Benutzerführung auf der LCD-Anzeige wurde um ein Menü zur Firmware-Aktualisierung erweitert. Dieses Menü erlaubt das Einspielen einer neuen Firmware von einem angeschlossenen USB-Speichermedium. Dies ist vor allem für nur WLAN-Geräte von Vorteil. Wird ein USB-Speichermedium eingesteckt, dann erscheint ein Popup-Menü auf der LCD-Anzeige (Abbildung 18) mit ausgewählten Optionen zur schnellen Wahl, darunter Firmware-Upgrade und Backup.



Abbildung 18: LCD Popup-Menü für USB-Speicher

4.11 Neuigkeiten im L-IP 6.1.0

Dieser Abschnitt beschreibt wichtige Änderungen und neue Funktionen. Eine vollständige Liste der Änderungen finden Sie in der Liesmich-Datei.

Neue L-IP Modelle

Die neuen L-IP Modelle, deren Produktbezeichnung auf „C“ endet werden jetzt unterstützt. Ausgestattet mit einer LCD-Anzeige, Dual-Ethernet und einer eingebauten Firewall stellen diese Modelle einen kompatiblen Ersatz für Modelle der B-Serie dar. Zusätzlich unterstützen sie auch noch die WLAN-Technologie.

Projektdokumentation

Eine neue Funktion ist das Web-Interface zum Erstellen und Ansehen von Projektdokumentation auf dem Gerät. Der Dokumentations-Editor benötigt Administrator-Rechte und erlaubt das Speichern von Dateien auf dem Gerät sowie das Erstellen von Querverweisen (Links auf URLs) zur Dokumentation. Beide Einträge können vom Guest-Benutzer jederzeit aufgerufen werden. Damit können beispielsweise Verkabelungspläne als PDF abgelegt werden oder Links auf eine Web-Seite erstellt werden, die Benutzerhandbücher oder andere hilfreiche Projektdokumentation enthält. Lesen Sie in Abschnitt 7.6.3 mehr über Projektdokumentation am Gerät.

Dual-Ethernet mit separaten Netzwerken

L-IP Modelle der C-Serie mit zwei Ethernet-Interfaces können so konfiguriert werden, dass sie auf zwei separaten, isolierten IP-Netzen arbeiten. Es kann zum Beispiel auf ein Ethernet-Interface über HTTPS von einem WAN aus zugegriffen werden, das auf Ethernet 2 angeschlossen ist, während die Dienste im Gebäudenetz lokal auf dem LAN laufen, das mit Ethernet 1 verbunden ist. Für die Konfiguration bietet das Gerät separate Ethernet-Reiter in der Port-Konfiguration, auf denen pro Interface die jeweils verfügbaren Dienste konfiguriert werden können. Im Beispiel aus Abbildung 19 wird das WAN-Interface nur mit HTTPS und OPC UA konfiguriert, während CEA-709 over IP (CEA-852) weiterhin auf Ethernet 1 (LAN) gebunden ist. Für weiterführende Information über die Verwendung von mehreren Ethernet-Ports lesen Sie bitte den Abschnitt 7.3.4.

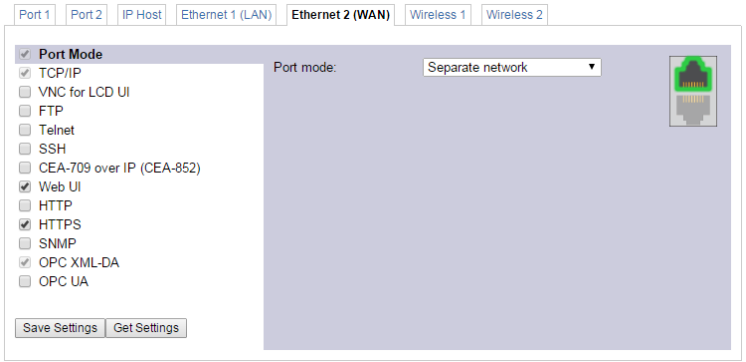


Abbildung 19: Neuer Reiter Ethernet 2 (WAN)

WLAN-Interface

In Kombination mit dem externen Interface LWLAN-800 bietet das Gerät weitere neue Interface-Reiter für drahtlose IP-Netze (WLANs). So wie beim zweiten Ethernet-Interface kann ausgewählt werden, welche einzelnen Protokolle über das WLAN verfügbar sein sollen. Das WLAN-Interface kann zum Betrieb als WLAN-Client, Access Point oder Mesh-Knoten konfiguriert werden. Mit letzterem kann ein drahtloses, vermaschtes Netzwerk aus LOYTEC-Geräten aufgebaut werden. Bitte lesen Sie den Abschnitt 7.3.8, um mehr über das WLAN-Interface zu erfahren.

SNMP

Um vitale Betriebsparameter in einer üblichen IT-Ausstattung auslesen zu können, bieten L-IP Geräte der C-Serie eine SNMP Management Information Base (MIB) an. Alle System-Register sind in dieser MIB abgebildet. Die MIB-Datei kann vom Gerät geladen und in ein SNMP Management Tool importiert werden. Alarme auf dem Gerät können als SNMP Traps verfügbar gemacht werden. Für weitere Information zur Konfiguration und Verwendung von SNMP auf einem LOYTEC Gerät lesen Sie bitte den Abschnitt 11.1.

OPC UA Server

Die L-IP Modelle der C-Serie sind mit einem OPC-Server ausgestattet, der sowohl OPC XML-DA als auch OPC UA unterstützt. Mit dem OPC-Server integriert sich das Gerät perfekt in die Geräteverwaltung der LWEB-900 Gebäudemanagement-Software.

Wireshark Paketaufzeichnung

Die L-IP Modelle der C-Serie besitzen die Funktion einer Wireshark Paketaufzeichnung. Mit dieser Funktion können Protokollaufzeichnungen gemacht und am L-IP abgelegt werden. Es ist auch möglich, den Wireshark Protokollanalysator am PC mit dem L-IP zu verbinden und eine Live-Aufzeichnung von Paketen laufen zu lassen. Lesen Sie dazu bitte den Abschnitt 14.9.

5 Quick-Start Anleitung

Dieses Kapitel gibt Schritt für Schritt Anweisungen, wie der L-IP in einem einfachen Netzwerk in einer LAN-Umgebung zu konfigurieren ist.

5.1 Hardware Installation

5.1.1 L-IP

Schließen Sie ein erdfreies, galvanisch getrenntes 20-30 VAC/VDC Netzteil an, verbinden Sie das CEA-709 Netzwerk sowie das Ethernet-Kabel wie im Installationsblatt dargestellt. Detaillierte Anweisungen finden Sie in Kapitel 6.

5.1.2 L-IP Redundant

Schließen Sie den Stromanschluss (12-35 VDC oder 12-24 VAC), das Ethernetkabel und das CEA-709 Kabel wie im Installationsblatt dargestellt. Abhängig vom gewünschten Betriebsmodus wählen Sie eine der Topologien zur Verkabelung gemäß Abbildung 20 bis Abbildung 22. Eine ausführliche Beschreibung folgt in Kapitel 6.

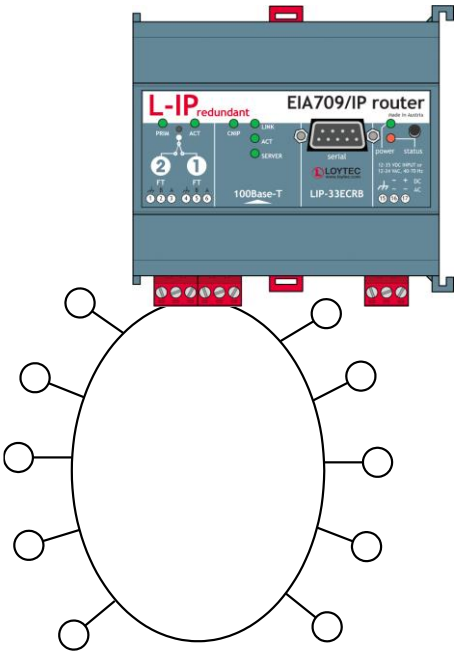


Abbildung 20: L-IP Redundant als Einzelgerät mit Bus Loop Monitoring

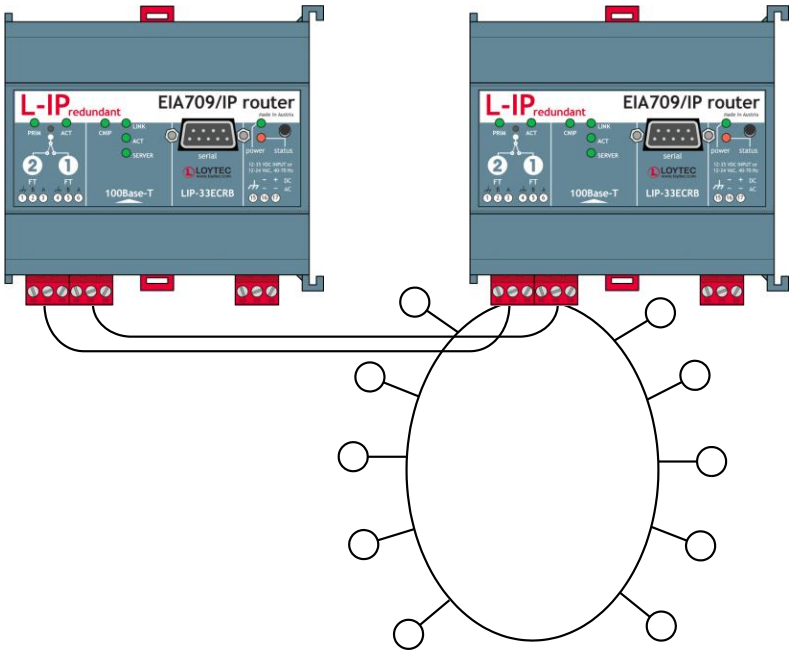


Abbildung 21: L-IP Redundant im „Twin Router“ Modus mit Bus Loop Monitoring

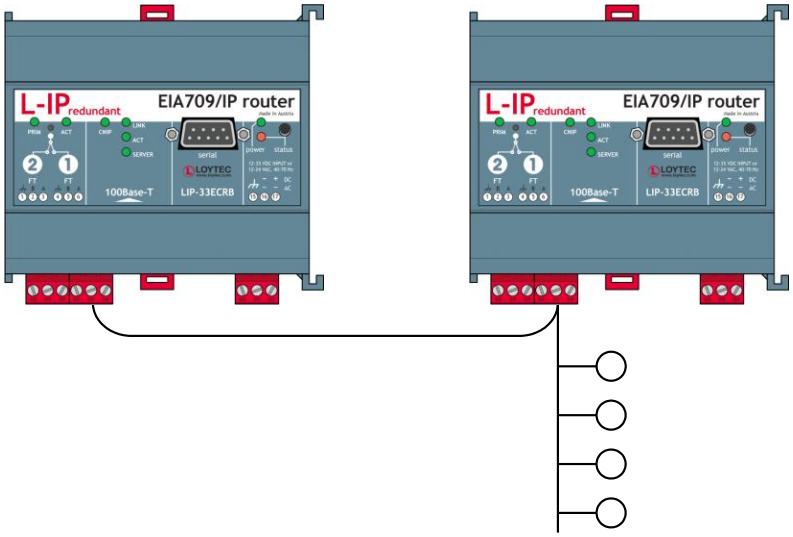


Abbildung 22: L-IP Redundant im „Twin Router“ Modus ohne Bus Loop Monitoring

5.2 IP Konfiguration eines Client-Geräts

5.2.1 Konfiguration auf dem Web-Interface

LOYTEC-Geräte werden mit DHCP ausgeliefert und beziehen automatisch eine IP-Adresse, sobald sie an ein Netzwerk angeschlossen werden. Um eine statische IP zu verwenden, kann das Web-Interface zur Konfiguration des Geräts verwendet werden. Geben Sie in einem Webbrowser die IP-Adresse des Geräts ein, welche auf der LCD-Anzeige steht. Beachten Sie dabei, dass der PC am selben Subnetz wie das Gerät angeschlossen sein muss.

Um eine statische IP einzustellen:

1. Öffnen Sie Ihren Webbrowser und geben Sie die IP-Adresse ein, welche auf der LCD-Anzeige steht oder tippen Sie ‚loytec.local' ein. Als erster Schritt werden Sie aufgefordert, Passworte für das Admin und Operator-Konto einzugeben, bevor Sie weitermachen können. Es werden nur starke Passworte akzeptiert.



Abbildung 23: Geben Sie Passwort für Admin und Operator-Konten ein.

2. Dann klicken Sie auf das **Config**-Menü. Klicken Sie auf **Port Config** im Config-Menü und wechseln Sie auf den Reiter **Ethernet**. Die TCP/IP-Eigenschaften sind markiert, wie in Abbildung 24 gezeigt. Geben Sie die IP-Adresse, die IP-Netzmaske und das IP-Gateway für das Gerät ein.

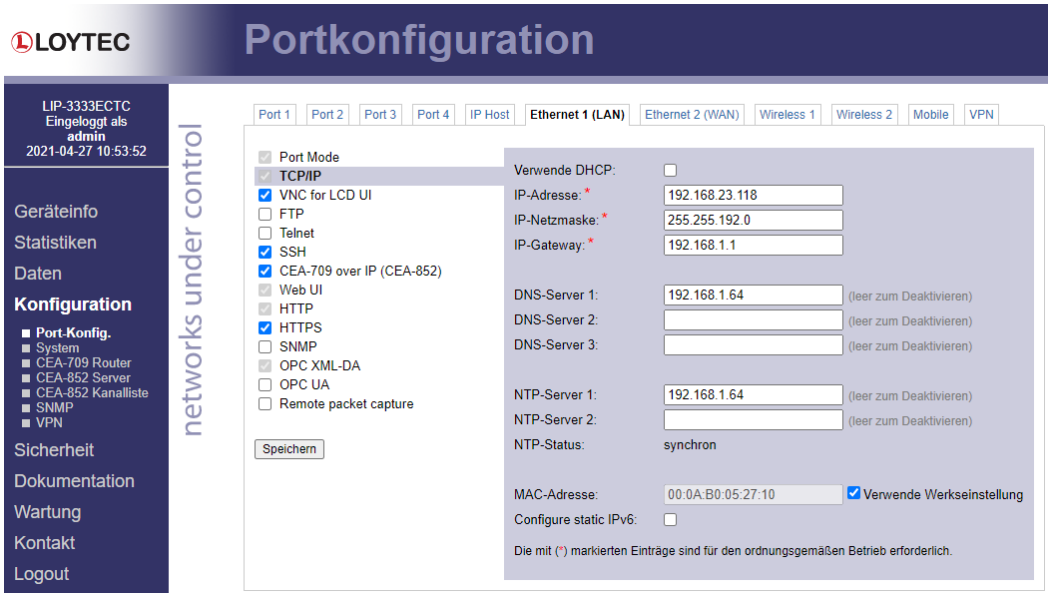


Abbildung 24: Geben Sie die IP Adresse und die Gateway Adresse ein

3. Klicken Sie auf **Save Settings** und starten Sie danach das Gerät neu, indem Sie auf Reset im hervorgehobenen Text klicken. Dies ändert die IP-Einstellungen des Geräts.

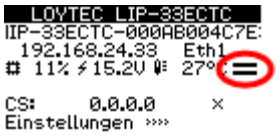
5.2.2 Configuration über das LCD-Display

Auf Gerätemodellen mit einem LCD-Display können die Basiseinstellungen auch über die Navigation durch Dreh-/Drückbedienung am Gerät selbst gemacht werden. Drehen sie hierzu

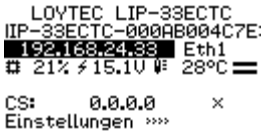
das Rad um zwischen den Menüs zu wechseln und drücken Sie es, um in den Einstellungsmodus zu wechseln. Befinden Sie sich im Einstellungsmodus können Sie Werte durch Drehen verändern und durch erneutes Drücken einstellen. Einige Eingabefelder berücksichtigen die Beschleunigung. Das bedeutet, dass größere Werteänderungen vorgenommen werden, wenn schneller gedreht wird.

Um die IP-Adresse über das LCD-Display einzustellen

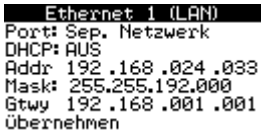
1. Setzen Sie die gewünschte Sprache auf der LCD-Hauptseite. Wählen Sie dazu das Flaggen-Symbol an und drücken den Knopf. Wählen Sie dann die gewünschte Sprache aus.



2. Navigieren Sie auf der LCD-Hauptseite zur IP-Adresse und drücken Sie den Knopf.



3. Navigieren Sie darin zu den benötigten Eingabefeldern, drücken und ändern die Werte. Setzen Sie die Werte jeweils durch erneutes Drücken und navigieren Sie zum nächsten Feld.

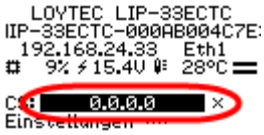


4. Schließlich navigieren Sie zu **Übernehmen** und drücken den Knopf.

5. Bestätigen Sie die Sicherheitsabfrage und das Gerät startet mit der neuen IP-Adresse.

Um bei einem Configuration Server zu registrieren

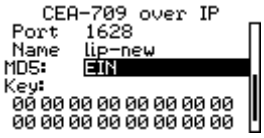
1. Auf der LCD-Hauptseite navigieren Sie auf das Adress-Feld neben CS und drücken Sie darauf.



2. Das bringt Sie zum Menü **CEA-709 over IP**. Navigieren Sie zur **Config Server IP** und geben dort die IP-Adresse in die vier Felder ein. Optional verändern Sie noch den **Config Server Port**.



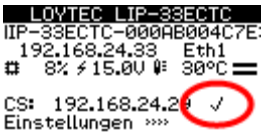
3. Falls der Kanal die MD5-Authentifizierung erfordert, setzen Sie MD5 auf **EIN** und geben Sie den geheimen Schlüssel darunter ein.



4. Schließlich navigieren Sie and Ende der Seite, drücken auf **Speichern** und bestätigen dies mit **JA**. Das Gerät versucht nun, sich beim Configuration Server zu registrieren. Beobachten Sie dabei die Status-Information, bis der Vorgang beendet.



5. Zurück auf der Hauptseite wird der Configuration Server mit einem Haken angezeigt.



5.3 Konfigurationsserver-Einstellungen

Sollte der L-IP auch als Konfigurationsserver für den CN/IP-Kanal dienen, öffnen Sie das Web-Interface und gehen zum Menü **CEA-852 Server**. In der Auswahlliste **Config server status** wählen Sie **enabled** und drücken auf **Save Settings** um den Konfigurationsserver zu aktivieren. Danach werden alle Einstellungen zum Konfigurationsserver auf dieser Seite angezeigt.

Dann gehen Sie zum Menü **CEA-852 Ch. List** und drücken den Knopf **Add Device**, um ein neues CEA-852-Gerät hinzuzufügen. Geben Sie dafür einen Namen und die IP-Adresse ein und drücken den Knopf **Save**, wie in Abbildung 25 dargestellt. Bei den Client-Geräten handelt es sich unter anderem um alle anderen L-IPs und PCs, die an der Kommunikation am IP-852 Kanal teilnehmen sollen.

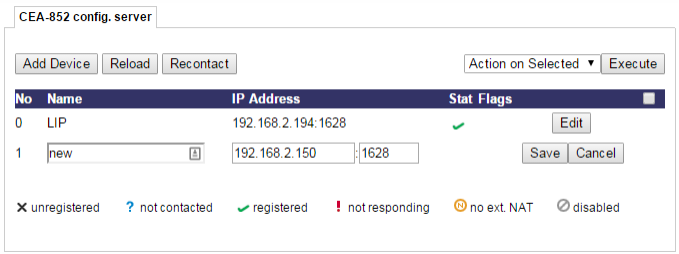


Abbildung 25: Hinzufügen eines Client-Geräts zum einem Kanal.

Nachdem Sie alle Client-Geräte in die Kanalliste aufgenommen haben, überprüfen Sie in der Kanal-Liste, dass alle Geräte erfolgreich am Konfigurationsserver registriert wurden und einen grünen Haken zeigen. Die CNIP-LED sollte nun auf allen Geräten grün leuchten, die eine solche besitzen, und die Server-LED am Konfigurationsserver L-IP sollte ebenfalls grün leuchten. L-IP Geräte mit einer LCD-Anzeige werden die Adresse des Konfigurationsservers anzeigen (oder LOKALER CS) und ein Häkchen aufweisen, wenn sie korrekt bei einem Konfigurationsserver registriert sind, wie in Abbildung 26 gezeigt.

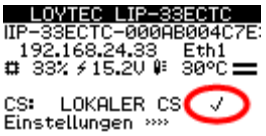


Abbildung 26: L-IP LCD-Anzeige für einen registrierten CEA-852-Client.

Fügen Sie nun die L-IP Router zu Ihrer Netzwerkzeichnung hinzu und kommissionieren die L-IPs. Bitte beachten Sie, dass wir Shapes für LonMaker auf unserer Homepage zur Verfügung stellen. Sie sollten nun im Stande sein, über den Ethernet-Kanal hinweg mit Ihren CEA-709-Komponenten zu kommunizieren. Detaillierte Informationen zur Konfiguration des Konfigurationsservers erhalten Sie in Abschnitt 7.3.14.

5.4 Konfiguration als Drop-In-Ersatz für LON-Router

Ein Multiport-L-IP (z. B. LIP-13ECTC oder LIP-33ECTC) kann als Drop-In-Ersatz für LON-Router von Drittanbietern konfiguriert werden, die zwischen TP-1250/FT-10 bzw. FT-10/FT-10 routen. Gehen Sie dazu zum LCD-Menü **Einstellungen »»** und navigieren Sie zu **CEA-709 »» Router Modus »»**.

Wählen Sie den **Modus** „Smart Switch“ und den Geräte-**Type** „L-Switch“ und wählen Sie dann **Speichern und neu starten** (siehe Abbildung 27). In dieser Einstellung fungiert das Gerät als selbstlernender Router zwischen den beiden CEA-709-Ports, während IP-852 deaktiviert ist. Im Smart Switch™-Routermodus ist keine Neukonfiguration in der LNS-Datenbank erforderlich. Wenn der Router in LNS sichtbar sein muss, wählen Sie stattdessen den Modus „Conf. Router“.



Abbildung 27: Router Mode-Menü auf der LCD-Bedienung.

Die IP-Einstellungen sind in diesem Betriebsmodus nicht erforderlich. Für Firmware-Upgrades und andere Gerätewartungsvorgänge über die Weboberfläche wird jedoch empfohlen, auch die IP-Adresse einzurichten.

5.5 L-IP Redundant Konfiguration

Der L-IP Redundant muss als Configured Router betrieben werden und erfordert daher die Kommissionierung mit einer Netzwerkmanagementsoftware. Der Smart Switch Modus, Repeater Modus oder Bridge Modus werden nicht unterstützt!

In der Werkseinstellung unterstützt der L-IP Redundant das Bus Loop Monitoring (siehe Abbildung 20). Zum Betrieb im Twin Router Modus (siehe Abbildung 21) müssen zusätzliche Einstellungen vorgenommen werden:

- Fügen Sie ein Router Shape für jeden L-IP Redundant in ihr Projekt ein. Verbinden Sie beide Router mit demselben IP-Kanal auf der einen und demselben FT-10 Kanal auf der anderen Seite.

- Fügen Sie je einen L-IP Redundant Überwachungsknoten „L-IP Redundant Diagnostic FT-10“ für die beiden Router auf dem TP/FT-10 Kanal ein. Die zugehörige Gerätevorlage (Device Template) wird zusammen mit dem L-IP Redundant Plug-In installiert, dass von der LOYTEC Webpage http://www.loytec.com geladen werden kann.

- Fügen Sie einen „Twin Router“ Funktionsblock für jeden der beiden L-IP Redundant Diagnostic Knoten ein.

- Verbinden Sie die Netzwerkvariable *nvoRedRtr* des einen L-IP Redundant mit der Variable *nviRedRtr* des anderen L-IP Redundant und umgekehrt.

Bei Verwendung von LonMaker for Windows sollte das Ergebnis wie in Abbildung 28 aussehen. Die PRIM LED eines der beiden L-IP Redundant Geräte muss grün leuchten, die LED des anderen Gerätes muss ausgeschaltet sein.

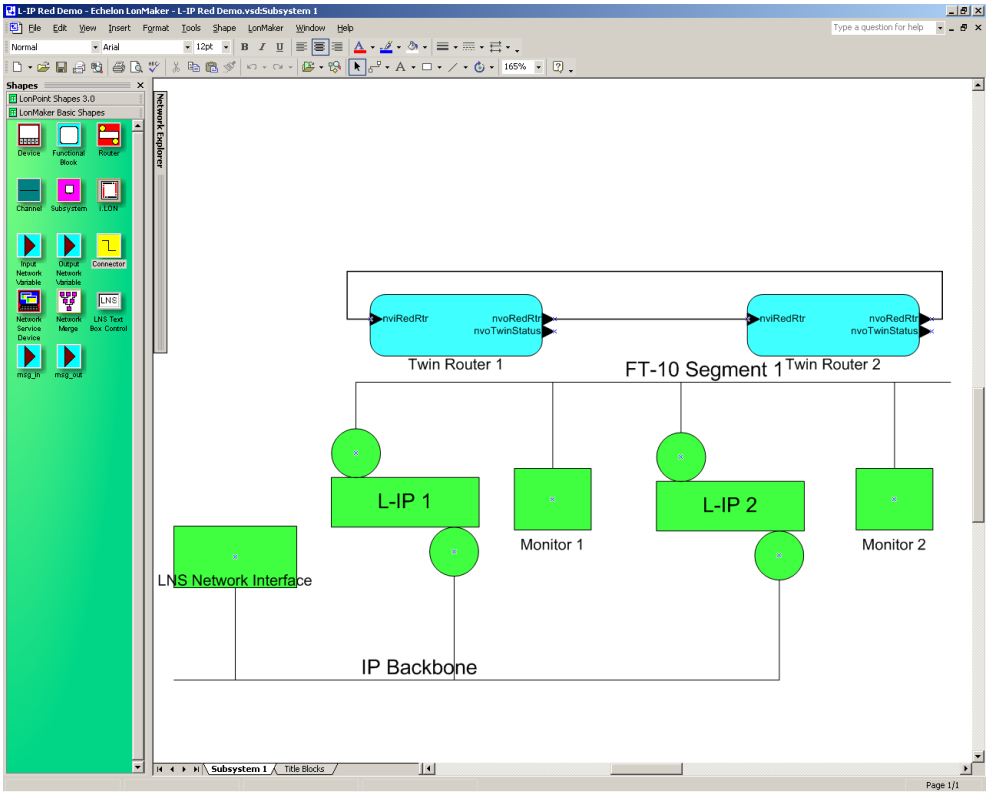


Abbildung 28: Ein Paar von L-IP Redundant Routern, konfiguriert im Twin Router Modus

Eine ausführliche Beschreibung der Konfiguration des L-IP Redundant finden Sie in Kapitel 10.

6 Hardware Installation

6.1 Gehäuse

Das Gehäuse des Produkts und seine Anschlüsse werden im Installationsblatt beschrieben, das dem Produkt in der Schachtel beiliegt.

6.2 Produkt-Label

Das Produkt-Label auf der Seite des L-IP beinhaltet folgende Informationen.

- L-IP-Bestellnummer mit Barcode (z.B. LIP-3ECTC, LIP-33ECTC oder LIP-3ECRB)
- Seriennummer mit Barcode (SER#)
- Eindeutige Node-ID und Virtual-ID für jeden Port (NIDx and VIDx)
- Ethernet MAC ID mit Bar-Code (MAC1).

Sofern nicht anders angegeben, sind alle Bar-Codes mit "Code 128" kodiert. Ein zusätzliches Label wird außerdem zu Dokumentationszwecken mitgeliefert. Die genauen Angaben auf dem Produkt-Label werden am Installationsblatt ausgewiesen, das dem Produkt in der Schachtel beiliegt.

Eine Virtual-ID (VID) bezeichnet eine Node-ID (NID) am IP Kanal. Intern verwenden die 2-Port (LIP-xxECTB, LIP-xxECTC) und die 4-Port (LIP-xxxxECTB, LIP-xxxxECTC) Varianten des L-IP bis zu 5 einzelne Router, die über einen TP/XP-1250 Backbone verbunden sind (siehe Abbildung 29 und Abbildung 31). Auf dem Label am Gerät sind nur die externen NIDs (Nummer 1-3 oder 1-5) aufgedruckt. Weil die NIDs in einem zusammenhängenden Block organisiert sind, können die internen NIDs abgeleitet werden, indem die aufgedruckten Nummern weitergezählt werden (Nummer 4-6 oder 6-10, siehe Abbildung 30 und Abbildung 32).

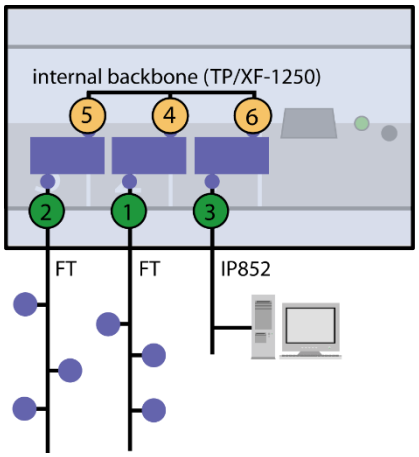


Abbildung 29: Interne Zuordnung von NIDs am LIP-xxECTB.

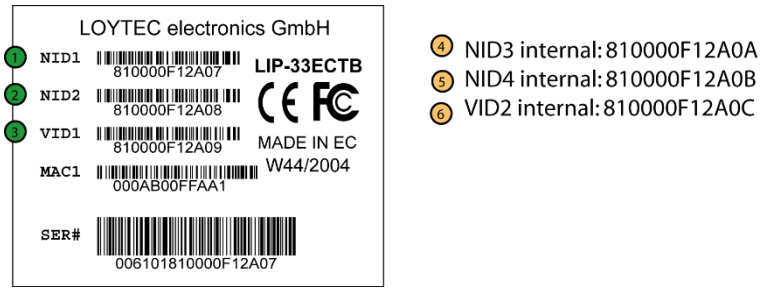


Abbildung 30: Beispiel für die Anordnung der internen NID am LIP-xxECTB.

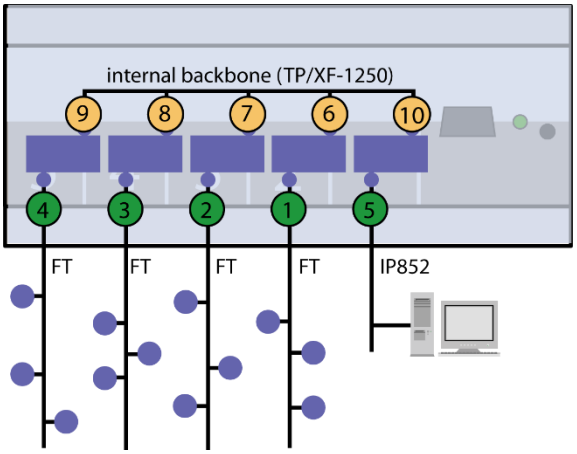


Abbildung 31: Interne Zuordnung von NIDs am LIP-xxxxECTB.

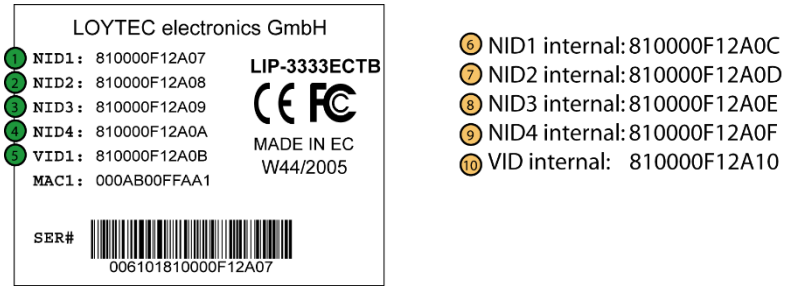


Abbildung 32: Beispiel für die Anordnung der internen NID am LIP-xxxxECTB.

6.3 Montage

Das Gerät verfügt über eine Halterung zur einfachen und schnellen Rastmontage auf Normschienen nach DIN EN 50 022. Der L-IP wird per Rastmontage auf einer entsprechenden Schiene befestigt. Die Einbaulage ist in beiden Fällen beliebig. Es ist jedoch auf eine ausreichende Belüftung zur Einhaltung des spezifizierten Temperaturbereichs zu achten.

6.4 Signal LEDs

Die verfügbaren LEDs und deren Position am Gehäuse werden im Installationsblatt ausgewiesen, das dem Produkt in der Schachtel beiliegt.

6.4.1 Power LED

Die L-IP Power LED leuchtet grün, wenn Strom an die Klemmen 24, 25 und 26 angelegt wird.

6.4.2 Status LED

Der L-IP hat eine rote Status LED (siehe Installationsblatt). Diese LED ist normalerweise dunkel. Falls das Fall-Back Image geladen wurde blinkt die LED einmal pro Sekunde rot.

6.4.3 CEA-709 Activity LED

Der CEA-709 Port am L-IP hat eine dreifärbige LED (grün, rot und orange, siehe (siehe Installationsblatt). Tabelle 2 zeigt die möglichen LED-Modi und ihre Bedeutung.

Verhalten	Bedeutung	Kommentar
GRÜN schnell blinkend	Netzwerkverkehr	
GRÜN blinkend mit 1 Hz	Port unkonfiguriert	Nur wenn der L-IP als CEA-709 Router betrieben wird (siehe Abschnitt 8.1.1)
ROT permanent	Port beschädigt	
ROT schnell blinkend	Netzwerkverkehr mit hoher Fehlerhäufigkeit L-IP Redundant: Ring offen (siehe Abschnitt 6.4.10)	
ROT blinkend mit 1Hz (alle Ports)	Firmwareimage korrupt Bitte laden Sie eine neue Firmware	
ORANGE permanent	Port deaktiviert	z.B. mittels LSD Tool (siehe Kapitel 15)
ORANGE schnell blinkend	Netzwerkverkehr auf einem als Management-Port konfigurierten Port	z.B. mittels LSD Tool (siehe Kapitel 15)
ORANGE blinkend mit 1 Hz	Automatische Bitratenerkennung	Nur RS-485 Ports
ORANGE permanent (alle Ports)	Statustaster wurde mehr als 20 Sekunden gedrückt gehalten Sobald der Statustaster ausgelassen wird, werden die Forwarding-Tabellen rückgesetzt	Nur im Betriebsmodus „Smart Switch“ oder „Repeater“

Tabelle 2: Port LED Anzeigen.

6.4.4 Twin Router Status LED (Nur L-IP Redundant)

Der L-IP Redundant ist mit einer drei Farben LED ausgestattet (grün, rot und orange, siehe (siehe Installationsblatt) die den Twin Router Status anzeigen. Diese LED ist mit „PRIM“ gekennzeichnet. Tabelle 3 zeigt die verschiedene LED Verhalten und deren Bedeutung.

Verhalten	Beschreibung	Kommentar
GRÜN	Gerät ist aktiv	Einzelgerätemodus oder primäres Gerät im Twin Router Modus
AUS	Gerät ist inaktiv	Sekundäres Gerät im Twin Router Modus
ORANGE	Gerät ist aktiv, aber es wurde ein Problem mit dem Twin Router erkannt	Primäres Gerät: Sekundäres Gerät nicht erreichbar Sekundäres Gerät: Primäres Gerät nicht erreichbar, Gerät hat die Rolle des primären Routers übernommen
ROT	Gerät ist inaktiv, da ein Fehler erkannt wurde	Gerät ist primäres Gerät, aber sekundäres Gerät hat die Funktion übernommen

Tabelle 3: Twin Router Status LED Anzeigen

Zur Aktivitätsanzeige flackert die LED kurz, wenn der L-IP Redundant seinen Twin Router kontaktiert.

6.4.5 Ethernet Link LED

Die Ethernet Link LED leuchtet grün, wenn ein Ethernetkabel angesteckt ist und eine Verbindung mit einem Switch, Hub, oder PC besteht.

6.4.6 Ethernet Activity LED

Die Ethernet Activity LED leuchtet grün für 6ms, wenn ein Paket gesendet oder empfangen wurde oder wenn eine Kollision am Netzwerkkabel detektiert wurde.

6.4.7 CEA-852 Status LED (CNIP LED)

Die CNIP LED ist eine dreifärbige LED, die unterschiedliche Betriebszustände des L-IP anzeigt.

Grün: Das Gerät ist voll funktionsfähig und alle CNIP Konfigurationsdaten (Channel-Routing-Info, Channel-Membership-List, Send-List) sind aktuell.

Grün blinkend: Falls ein gültiges CEA-709 Paket am IP Kanal empfangen oder gesendet wird, schaltet sich die CNIP LED für 50 ms aus. Nur gültige CEA-852-Pakete, die an die IP Adresse des L-IP gesendet werden, können angezeigt werden. Verworfene Pakete oder nicht an den L-IP adressierte Pakete werden nicht angezeigt. Dieses Verhalten der CNIP LED ist erst seit Firmwareversion 1.1 verfügbar.

Orange: Das Gerät funktioniert aber einige CNIP Konfigurationsdaten sind nicht aktuell (das Gerät kann den Konfigurationsserver nicht erreichen arbeitet jedoch mit Konfigurationsdaten die im Flash gespeichert sind). Die LED blinkt gelb, wenn Aktivität am Netzwerk besteht.

Rot: Das Gerät ist nicht betriebsbereit, da es vom CN/IP Kanal zurückgewiesen wurde oder es hat sich infolge eines internen Fehlers selbst abgeschaltet.

Aus: Das Gerät ist nicht betriebsbereit, da das CNIP Module nicht gestartet wurde. Dies kann der Fall sein, falls der L-IP den DHCP Service verwendet und er vom DHCP Server keine gültige IP Konfiguration (Adresse) empfangen hat.

Rot blinkend mit 1 Hz: Das Gerät ist nicht betriebsbereit, da es keine Konfigurationsdaten erhalten hat. Bitte fügen Sie das Gerät dem CN/IP Kanal hinzu (Registrierung im Konfigurationsserver).

Grün oder orange blinkend mit 1 Hz: Der Router des CN/IP Ports wurde noch nicht kommissioniert. Die Farbe der LED zeigt weiterhin den Status des Geräts im CN/IP-Kanal an.

6.4.8 Konfigurationsserver LED

Die Konfigurationsserver LED leuchtet grün, wenn der Konfigurationsserver am L-IP aktiviert wurde.

6.4.9 Wink-Aktion

Wenn der L-IP auf einem seiner Netzwerkports ein Wink-Kommando empfängt, wird dies durch ein Blinkmuster auf der CNIP und der CEA-709 Activity LED angezeigt. Die CNIP und die CEA-709 Activity LED leuchten abwechselnd grün/orange/rot (jeweils 0.15s). Dieses Blinkmuster wiederholt sich 6-mal. Anschließend leuchtet die CNIP LED 6 mal orange falls das Wink-Kommando am IP Kanal empfangen wurde oder es leuchtet die CEA-709 Activity LED 6 mal orange falls das Wink-Kommando am CEA-709 Kanal empfangen wurde. Abschließend kehren alle LEDs in den normalen Betriebszustand zurück.

6.4.10 Netzwerk Diagnose

Der L-IP stellt mittels seiner CEA-709 Activity LED Diagnosemöglichkeiten zur Verfügung:

- Falls die LED nicht aufleuchtet ist dieses Port mit keinem Netzwerksegment verbunden oder es herrscht gerade kein Netzwerkverkehr auf diesem Segment vor.
- Wenn die LED grün aufblinkt, so zeigt dies ein funktionsfähiges Netzwerksegment an.
- Wenn die LED rot aufblinkt, so zeigt dies ein potentielles Problem auf diesem Netzwerksegment an. Dieser Betriebszustand wird als Überlastsituation bezeichnet.

Eine Überlastsituation kann auftreten, wenn

- die durchschnittliche Bandbreitenauslastung dieses Ports über 70 % liegt, oder
- die Kollisionsrate über 5 % liegt, oder
- mehr als 15% CRC-Fehler auf einem Power-Line-Kanal oder mehr als 5 % CRC-Fehler auf einem nicht Power-Line-Kanal aufgetreten sind.
- der L-IP es nicht geschafft hat alle Pakete zu verarbeiten.
- Der L-IP Redundant hat einen offenen Ring erkannt (nur L-IP Redundant, siehe Abschnitt 10).

Für eine bessere Fehlerabgrenzung der Überlastsituation wird empfohlen, einen Protokollanalysator (z.B. LOYTEC's LPA) zu verwenden. Der exakte Grund der Überlastsituation kann auch mit dem LSD Tool (siehe Kapitel 15) festgestellt werden.

Beim L-IP Redundant leuchtet die LED rot, wenn eine geöffnete Netzwerkschleife (Loop) erkannt wurde (siehe Kapitel 10).

6.5 Statustaster

Der L-IP ist mit einem Statustaster ausgerüstet (siehe (siehe Installationsblatt). Wenn der Statustaster kurz gedrückt wird, so sendet der L-IP eine "Service Pin Message" an beiden Netzwerkports. Bitte beachten Sie, dass jedes Port am L-IP seine eigene Node ID (Neuron ID) hat.

Wird der Multiport L-IP als CEA-709 Router betrieben (siehe Abschnitt 8.1.1) kann durch Drücken des Statustasters länger als 2 Sekunden der Port ausgewählt werden, von dem eine „Service Pin Message" Nachricht ausgesendet werden soll. Die Port-LED des gerade selektierten Ports leuchtet orange auf. Wird der Statustaster weiter gedrückt gehalten, so wird nach weiteren 2 Sekunden der nächste Port selektiert. Sobald der Statustaster freigegeben wird, wird von dem momentan selektierten Port/Router eine „Service Pin Message" Nachricht ausgesendet.

Wenn der Statustaster im Normalbetrieb für mehr als 20 s gedrückt wird, so werden die Forwarding-Tabellen des L-IP rückgesetzt.

6.5.1 Rücksetzen Forwarding Tabellen

Um die Forwarding-Tabellen rückzusetzen, muss der Statustaster für zumindest 20 Sekunden im Normalbetrieb gedrückt werden. Rücksetzen der Forwarding-Tabellen bedeutet:

- Löschen der Group-Forwarding-, der Subnet/Node-Forwarding- und der Router-Domain-Tabellen, wenn der L-IP im Switch Modus betrieben wird.

- Rücksetzen aller Ports auf den CEA-709 Status „unconfigured“.
- Löschen der L-IP Status- und Statistikdaten.
- Löscht **nicht** die IP Adresse und die CNIP (CEA-852) Konfigurationsdaten.

Die Rücksetzung erfolgt, wenn der Taster losgelassen wird. Anschließend wird das Gerät neu gestartet, um die neue Konfiguration zu aktivieren. Nachdem der Statustaster für mehr als 20 Sekunden gedrückt wurde leuchten die CEA-709 Activity LED und die CNIP LED orange auf und bleiben orange bis der Taster losgelassen wird und der L-IP startet neu.

Alternativ zum Drücken und Halten des Statustasters können die Forwarding-Tabellen im Menü **Geräteverwaltung** auf der LCD-Bedienung (siehe Abschnitt 6.6.1) zurückgesetzt werden.

Wichtig: ***Falls der L-IP von einem Ort im Netzwerk an einen andern Ort im Netzwerk bewegt wird oder größere Umstellungen im Netzwerk vorgenommen wurden, wird empfohlen, die Forwarding-Tabellen des L-IP rückzusetzen.***

Wichtig: ***Warten Sie mindestens 30 s nach dem Einschalten des Stromes bevor Sie den Statustaster drücken, um sicherzustellen, dass der L-IP vollständig gestartet ist!***

6.6 LCD-Anzeige und Dreh-/Drückrad

6.6.1 Geräteeinstellung

L-IP Gerätemodelle der C-Serie verfügen über eine LCD-Anzeige und bieten die Möglichkeit, die Basiseinstellungen über die LCD-Anzeige durch Dreh-/Drückbedienung vorzunehmen. Die Hauptseite der LCD-Anzeige ist in Abbildung 33 abgebildet. Hier werden vitale Informationen über das Gerät angezeigt, wie z.B. dessen IP-Adresse, der Host-Name, die CPU-Auslastung, die Systemtemperatur und die Betriebsspannung.

Im unteren Bereich befinden sich die Menüeinträge. Drehen Sie das Rad, um zwischen den Elementen zu navigieren und drücken Sie das Rad, um eine Auswahl zu treffen. Im Auswahlmodus drehen Sie das Rad, um Werte zu verändern, und drücken Sie erneut, um die Auswahl zu beenden.



Abbildung 33: Hauptseite der LCD-Anzeige

Das Menü **Einstellungen »»** erlaubt das Konfigurieren der Basiseinstellungen des Geräts. Navigieren Sie zu dem Untermenü **Geräteverwaltung »»** wie in Abbildung 34 gezeigt.



Abbildung 34: Geräteverwaltungsmenü auf der LCD-Bedienung

Dieses Menü enthält Optionen für die folgenden, grundlegenden Geräteeinstellungen:

- **TCP/IP Konfig**: Dieses Menü erlaubt die Einstellung der IP-Adresse des Geräts.

- **HTTP Server**: In diesem Menü kann der HTTP-Server ein- oder ausgeschaltet, sowie sein TCP-Port verändert werden.

- **HTTPS Server**: In diesem Menü kann der HTTPS-Server ein- oder ausgeschaltet, sein TCP-Port verändert und ein installiertes Zertifikat entfernt werden.

- **CEA-709 over IP**: In diesem Menü können die Einstellungen für den CNIP-Client vorgenommen werden, um diesen bei einem Konfigurationsserver zu registrieren. Siehe Abschnitt 6.6.3 für weitere Details.

- **Datum/Uhrzeit**: In diesem Menü kann die Uhrzeit eingestellt werden. Es ist möglich, einen Mechanismus zur Zeitsynchronisation zu wählen, und den UTC Offset und die Sommerzeit festzulegen.

- **Sende ID-Nachrichten**: Wenn dieses Menü angewählt wird, sendet das Gerät auf allen Ports Service-Pin, BACnet I-Am und Broadcast-Identifizierungs-Nachrichten aus. Die Identifizierungs-Nachrichten helfen das Gerät im L-Config Tool zu finden.

- **Konfig neu laden**: Durch Auswahl dieses Menüs lädt das Gerät Konfiguration neu. Dies ist schneller als einen kompletten Neustart durchzuführen.

- **Gerät neu starten**: Durch Auswahl dieses Menüs wird das Gerät vollständig neu gestartet.

- **Werkseinstellungen**: Durch Auswahl dieses Menüs wird das Gerät auf Werkseinstellung zurückgesetzt. Die IP-Adresse wird dabei ebenfalls gelöscht.

- **Remote Config**: Wird diese Option eingeschaltet kann der LWEB-900 Master Device Manager die zuletzt gesicherte Konfiguration auf das Gerät spielen, wenn es noch keine Konfiguration besitzt. Diese Option ist hilfreich, wenn das Gerät ausgetauscht wird, da nur noch die IP-Adresse auf dem neuen Gerät eingestellt werden muss.

- **PIN**: Ändern Sie den Standard-PIN auf eine beliebige 4-stellige Zahl, um bestimmte Operationen über die LCD-Bedienung zu schützen. Der Benutzer wird dann nach dem PIN für die geschützten Bereiche gefragt.

- **Kontrast**: Durch diese Einstellung kann der Kontrast des Displays adjustiert werden.

- **Sprache**: Wählen Sie hier die gewünschte Sprache in der LCD-Anzeige aus.

- **Forwarding-Tab. Rücks.**: Wählen Sie diesen Eintrag, um die Forwarding-Tabellen im Switch rückzusetzen.

6.6.2 Senden einer Node-Pin-Nachricht

Das Menü **Einstellungen »»** erlaubt auch die Basiseinstellung des CEA-709 Routers. Navigieren Sie zum Untermenü **CEA-709 »»** und wählen Sie eines der Router-Menüs aus, wie in Abbildung 35 gezeigt wird.



Abbildung 35: CEA-709 Router-Menü auf der LCD-Anzeige

In diesem Menü gibt es die folgenden Optionen für den gewählten CEA-709 Router-Port:

- **Send Nodepin**: Durch Auswahl dieses Menüs wird eine Node-Pin-Nachricht auf das CEA-709-Netzwerk gesendet.

- **NIDA, NIDB**: Diese Einträge zeigen die Node IDs der zwei Ports des gewählten Routers an.

- **State**: Dieser Eintrag zeigt an, ob der Router online oder offline ist.

6.6.3 CEA-852 Geräteeinstellung

Um die Einstellungen für das CEA-852 Gerät zu machen und bei einem Konfigurationsserver zu registrieren, navigieren Sie auf der Hauptseite zum Eintrag mit der IP-Adresse neben **CS:** und drücken Sie auf diese wie in Abbildung 36 gezeigt.

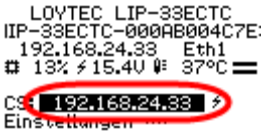


Abbildung 36: Einstellen der CS-Adresse auf der LCD-Anzeige.

Damit wird das Menü **CEA-709 over IP** geöffnet, das die folgenden Einstellungen bietet:

- **Config Server IP**: Geben Sie hier die IP-Adresse des Konfigurationsservers in die jeweiligen vier Felder ein.

- **Config Server Port**: Geben Sie hier den Port des Konfigurationsservers ein. Die Voreinstellung ist 1629, die in den meisten Fällen unverändert bleiben kann.

- **Config Client Port**: Geben Sie hier den Port des CEA-852-Clients ein. Die Voreinstellung ist 1628, die in den meisten Fällen unverändert bleiben kann.

- **MD5**: Die Voreinstellung ist aus. Stellen Sie MD5 ein, wenn der Kanal die MD5-Authentifizierung für die Sicherheit erfordert.

- **Key**: Wenn MD5 eingeschaltet ist, geben Sie in die folgenden 16 Felder den geheimen Schlüssel ein.

Auf der Hauptseite wird der Status der CEA-852 Einheit neben der CS-Adresse mit einem Symbol angezeigt. Dieser kann normal sein (✓), wartend auf einen Konfigurationsserver (⚡), oder noch nicht registriert (×). Wenn MD5 an ist, wird daneben noch ein Schlosssymbol 🔒 angezeigt.

6.6.4 Router Mode Einstellung

Das **Router Mode** Menü ist ein Untermenü der CEA-709 Einstellungen. Es erlaubt die Konfiguration folgender Basiseinstellungen für den Router:

- **Mode**: Diese Einstellung konfiguriert den Router-Betriebsmodus wie in Abschnitt 8.1 beschrieben:

    - Config. Router: Dies ist der Standardmodus für einen konfigurierten CEA-709-Router, der in der LNS-Datenbank in Betrieb genommen werden muss.

    - Smart Switch: Im Smart Switch™ Modus fungiert das Gerät als Plug-and-Play-selbstlernender Router, der keine LNS-Einrichtung benötigt.

    - Repeater: In diesem Modus ist das Gerät ein Store-and-Forward-Repeater.

- Switch (SN learn): Dieser Modus ähnelt dem Smart Switch™-Modus, aber nur das Subnetz-Lernen ist aktiviert und Subnetz-Broadcasts werden nicht geflutet (siehe Einzelheiten in Abschnitt 8.1).

- **Type**: Diese Einstellung definiert den grundlegenden Gerätetyp. „L-IP“ ist der Standardtyp und das Gerät fungiert als Router oder Smart-Switch™ zwischen den CEA-709-Ports (TP-1250 oder FT-10) und dem IP-852-Kanal. Als Typ „L-Switch“ fungiert das Gerät nur zwischen seinen CEA-709-Ports als Router und hat IP-852 deaktiviert.

Wenn der L-IP als Gerät vom Typ L-Switch im Smart Switch™-Modus konfiguriert ist, kann er als Plug-and-Play-Ersatz für gängige LON-Router von Drittanbietern verwendet werden.

6.7 Verkabelung

6.7.1 L-IP

Jeder L-IP CEA-709-Kanal ist mit einem Netzwerkabschluss gemäß der Spezifikation des entsprechenden Transceivers zu versehen (siehe Kapitel 12).

Wichtig: ***Alle Kanäle müssen ordnungsgemäß terminiert werden. LOYTEC empfiehlt zur Terminierung die LOYTEC L-Term Produkte (LT-13 bzw. LT-33). Auch bei nicht verwendeten CEA-709-Kanälen muss ein 100 Ohm Widerstand (mind. 0,25 Watt) als Abschluss zwischen den entsprechenden CEA-709 A und B Anschlüssen angebracht werden.***

Wichtig: ***Wenn Sie geschirmte Netzwerkkabel verwenden, so sollte nur eine Seite des Kabels mit Erde verbunden sein. Daher muss der Schirm entweder bei den L-IP-Anschlüssen oder anderswo im Netzwerk mit Erde verbunden sein (siehe Abbildung 37)!***

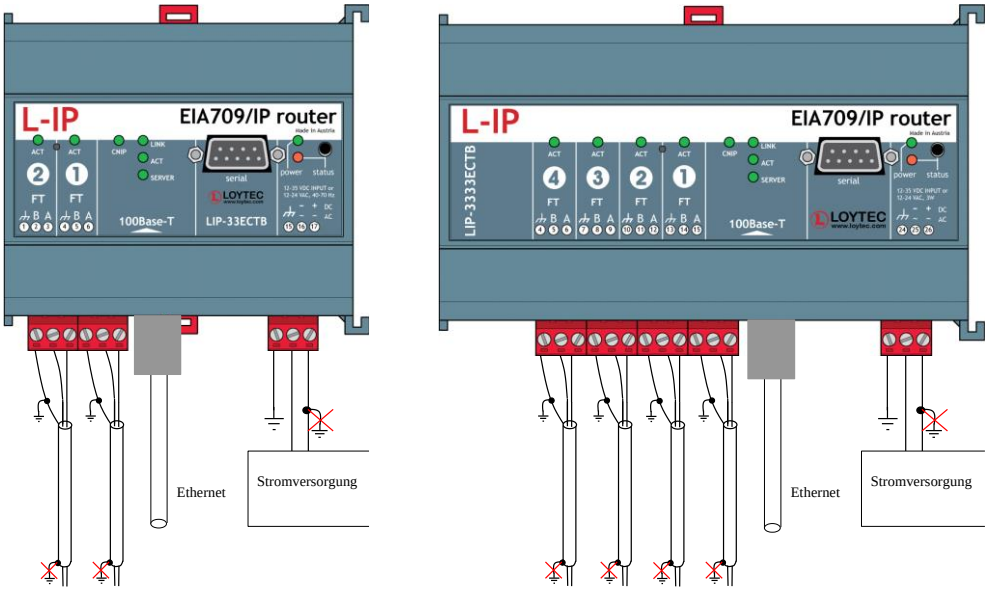
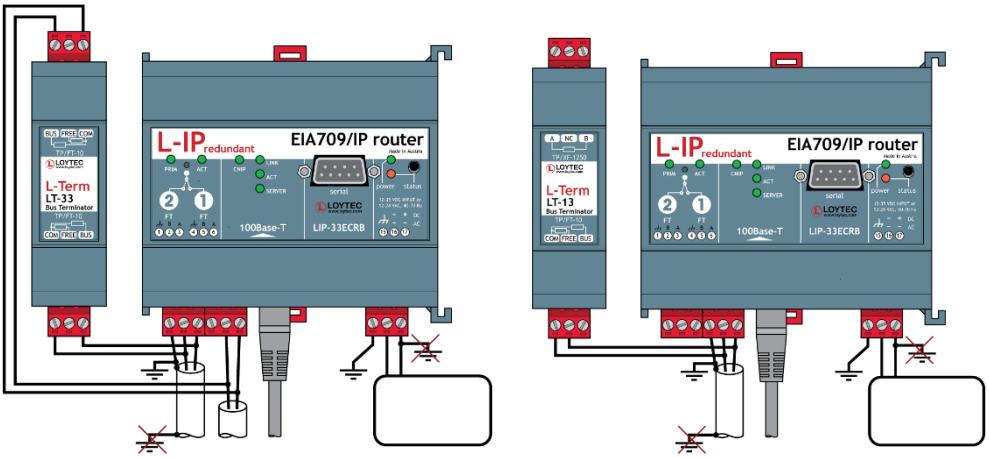


Abbildung 37: Verbindung der Erde zum L-IP der B-Serie.

6.7.2 L-IP Redundant

Jeder an den L-IP Redundant angeschlossene CEA-709-Kanal ist mit einem Netzwerkabschluss gemäß der Spezifikation des entsprechenden Transceivers zu versehen (siehe Kapitel 12).

Wichtig:	***Alle Kanäle müssen ordnungsgemäß terminiert werden. LOYTEC empfiehlt zur Terminierung die LOYTEC L-Term Produkte (LT-13 bzw. LT-33). Auch bei nicht verwendeten CEA-709-Kanälen muss ein 100 Ohm Widerstand (mind. 0,25 Watt) als Abschluss zwischen den entsprechenden CEA-709 A und B Anschlüssen angebracht werden.***



Bus loop monitoring enabled Bus loop monitoring disabled

Abbildung 38: : L-IP Redundant mit und ohne Bus Loop Monitoring

Wichtig:	***Wenn Sie geschirmte Netzwerkkabel verwenden, so sollte nur eine Seite des Kabels mit Erde verbunden sein. Daher muss der Schirm entweder bei den L-IP-Anschlüssen (Loop Seite 1) oder anderswo im Netzwerk mit Erde verbunden sein.***
Wichtig:	***Wenn Bus Loop Monitoring aktiviert ist (Loop Seite/Port 1 und Loop Seite/Port 2 angeschlossen), müssen beide Seiten der Schleife an den L-IP Klemmen terminiert werden (siehe Abbildung 38)! In diesem Fall sind zwei Terminatoren für Bustopologie erforderlich!***
Wichtig:	***Wenn Bus Loop Monitoring aktiviert ist darf sich zwischen Loop Port 1 und Loop Port 2 kein Repeater befinden!Console Interface***

7 Web Interface

Beginnend mit Firmwareversion 2.0 besitzt der L-IP einen eingebauten Webserver sowie ein Web-Interface, um das Gerät zu konfigurieren, Statistikinformationen abzurufen, die Gerätekonfiguration in eine Datei auf Ihrem PC zu sichern und eine abgespeicherte Konfiguration zurück ins Gerät zu laden. Mittels des Web-Interface können die IP-Einstellungen sowie die CEA-852-Geräteeinstellungen geändert werden sowie neue CN/IP-Geräte am CN/IP-Kanal angemeldet und entfernt werden. Das Web-Interface ist sehr leistungsfähig und intuitiv zu verwenden.

7.1 Geräteinformation und Benutzerkonten

7.1.1 Inbetriebnahme

Geben Sie in Ihrem Webbrowser die Standard IP Adresse 192.168.1.254 des L-IP ein. Bitte beachten Sie, dass wenn sich Ihr PC nicht im selben Subnet 192.168.1.xxx wie der L-IP befindet, sie folgenden route Befehle in einem Kommando-Fenster eingeben müssen, um eine Route zum L-IP festzulegen.

Um eine Route hinzuzufügen

1. Windows **START → Ausführen**
2. Geben Sie ‚cmd' ein und klicken Sie auf **OK**.
3. Im Konsolenfenster geben Sie folgende Kommandozeile ein

   ```
   route add 192.168.1.254 %COMPUTERNAME%
   ```

   Unter Windows7 geben Sie bitte die IP-Adresse des PCs anstelle von %COMPUTERNAME% ein.
4. Jetzt können Sie Ihren Webbrowser öffnen und die Standardadresse ‚192.168.1.254' eingeben.

Der Anmeldebildschirm des Geräts wird angezeigt und fordert Sie als erstes auf, die Passwörter für Administrator- und Operator-Konten festzulegen. Ein Indikator für die Passwortstärke informiert Sie über die Sicherheitsqualität Ihrer Passwörter. Geben Sie die Passwörter wie in Abbildung 39 gezeigt ein und klicken Sie dann auf **Passwörter setzen**.



Abbildung 39: Setzen der Passworte für admin und operator Konten.

Das Web-Interface kann nicht ohne vorheriges Setzen der Passwörter benutzt werden. Beachten Sie bitte, immer starke Passwörter zu verwenden (unter Vermeidung von ‚admin' oder ‚loytec4u'). Die Geräteinfo-Seite wird danach angezeigt. Die Passworte können später geändert werden, wie in Abschnitt 7.4.1 beschrieben.

7.1.2 Geräteinformation

Die Geräteinformationsseite (Abbildung 40) zeigt im Bereich **General Info** einige generelle Informationen über das Gerät an. Das beinhaltet das Modell und die gerade verwendete Firmwareversion. Darunter werden wichtige Betriebsparameter wie der freie Speicher, die CPU-Auslastung, die Systemtemperatur, die Betriebsspannung, den Status der Zeitsynchronisation und die Laufzeit angezeigt.

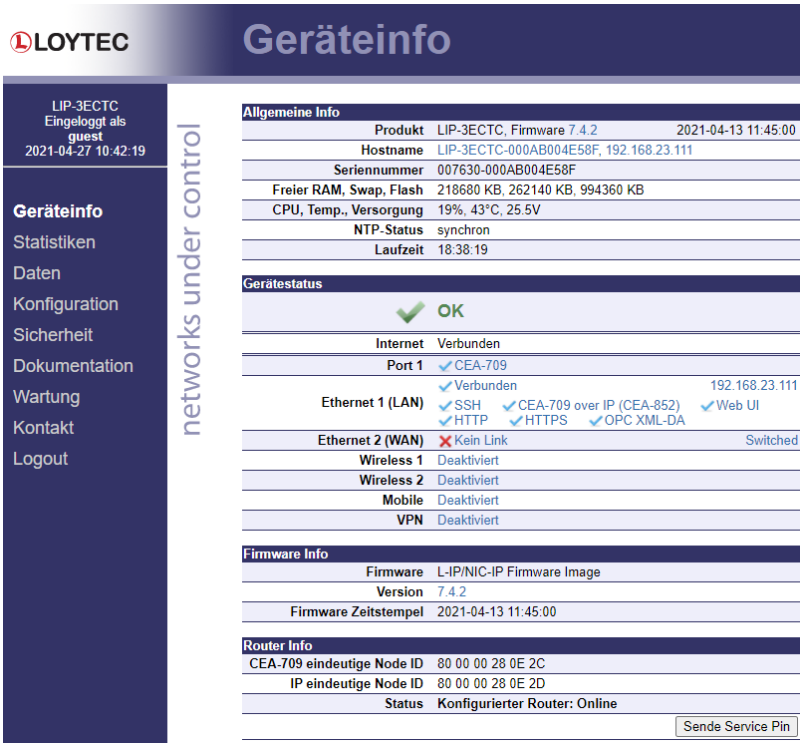


Abbildung 40: Beispiel für L-IP Startbildschirm

Der Abschnitt **Device Status** fasst den Status einzelner Ports und Protokolle am Gerät zusammen. Ein Summenstatus wird als grüner Haken gezeigt, wenn alles in Ordnung ist. Zeigten die Betriebsparameter eines Ports oder eines Protokolls einen abnormalen Zustand,

wird an dieser Stelle eine Warnung oder ein Fehlerzeichen dargestellt. Darunter wird eine Zusammenfassung der aktiven Protokolle auf den jeweiligen Ports angezeigt. Alle Einträge beinhalten einen Link auf die zugehörige Konfigurationsseite.

Unter den generellen Informationen stehen spezifischere Bereiche, die vom Modell abhängen. Die **Firmware Info** zeigt die Version und den Build-Zeitstempel von Primary- und Fallback-Image an, die am Gerät installiert sind.

Die Seite zeigt weiter noch die eindeutigen Node-IDs („Neuron IDs“) des CEA-709 Netzwerkinterfaces angezeigt. Der Multi-Port L-IP zeigt sowohl die externen Node-IDs als auch die internen Node-IDs am internen Backbone sparat an. Diese Seite kann auch dazu verwendet werden, um CEA-709-Service-Pin-Nachrichten zu senden. Dies ist beim Kommissionieren praktisch, da es dadurch nicht notwendig ist, vor Ort zu sein, um den Statustaster zu drücken.

7.1.3 Anmeldung am Gerät

Klicken Sie sich durch die Menüs auf der linken Seite, um sich mit den verschiedenen Seiten vertraut zu machen. Wenn Sie auf **Konfiguration** im linken Menü klicken, werden Sie aufgefordert, das Administratorpasswort einzugeben, um Änderungen an den Einstellungen vornehmen zu können, wie in Abbildung 41 gezeigt wird. Geben Sie das Administratorpasswort ein und klicken Sie auf **Login**.

Wenn Sie sich mit einem lokalen Benutzer mit der Rolle „admin“ anmelden, bearbeiten Sie den Benutzernamen im Feld **Account**.

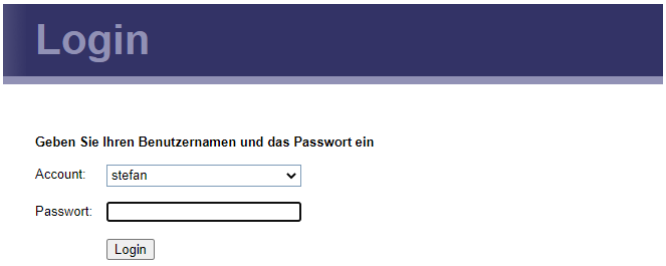


Abbildung 41: Geben Sie „loytec4u“ für das Administratorpasswort ein.

7.2 Gerätestatistik

Die Gerätestatistikseite bietet erweiterte Statistikinformation über die CEA-709-Einheit, CEA-852-Einheit, das Systemlog und das Ethernet-Interface an

7.2.1 System Log

Diese Seite zeigt alle Nachrichten an, die im Systemlog des Geräts gespeichert sind. Ein Beispiel ist in Abbildung 42 zu sehen. Diese Logdaten dienen zur Fehlersuche. Sie bestehen aus Logeinträgen bei Neustarts und ungewöhnlichen Betriebszuständen. Fehler und Warnings sind rot und gelb farbkodiert. Die voreingestellte Richtung zeigt die neuesten Einträge ganz oben an. Die Richtung kann durch einen Mausdruck auf den Pfeil ⇑ im Spaltenkopf umgestellt werden.

Um das Protokoll zu speichern, drücken Sie den Knopf **Save System Log**. Wenn Sie den LOYTEC Support bemühen, dann halten Sie eine Kopie dieses Logs bereit.

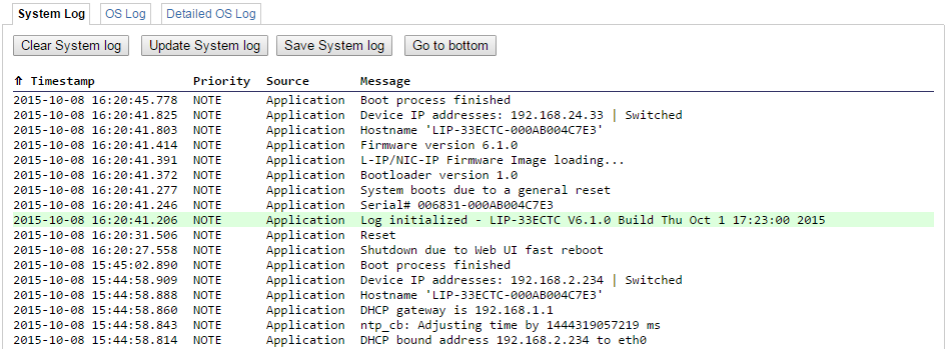


Abbildung 42: Systemlog

7.2.2 IP-Statistik

Abbildung 43 zeigt die IP-Statistikseite an. Auf der **Ethernet** Registerkarte können mögliche Probleme betreffend die IP-Kommunikation gefunden werden. IP-Adresskonflikte werden angezeigt (wenn die IP-Adresse des Geräts identisch mit der eines anderen Geräts am Netzwerk ist). Außerdem werden die Routing-Tabelle, die ARP-Tabelle (einschließlich IPv6 Neighbours), die DNS-Konfiguration und detaillierte Verbindungsstatistiken angezeigt. Die Registerkarte **Wireless** enthält Statistiken, die für die LWLAN-800-Schnittstelle spezifisch sind.

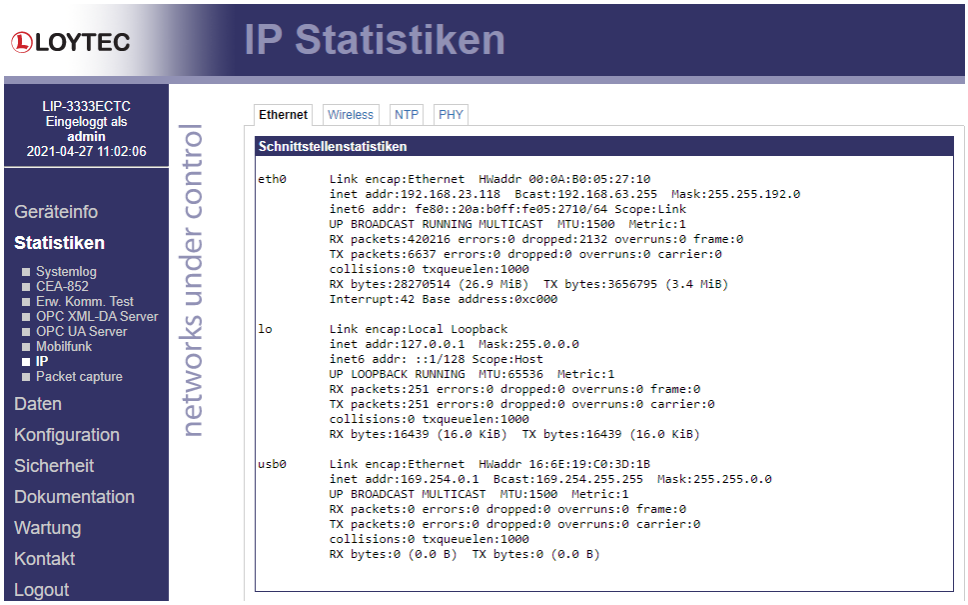


Abbildung 43: IP-Statistik.

Die Registerkarte **NTP** enthält Informationen zu den kontaktierten NTP-Servern und deren Synchronisierungsstatus. Auf der Registerkarte **PHY** werden Informationen zum Ethernet-Verbindungsstatus, zur Verbindungsgeschwindigkeit und zu den angezeigten MAC-Adressen an beiden Ethernet-Ports angezeigt.

7.2.3 CEA-852-Statistiken

Die CEA-852-Statistikseite zeigt die Statistik der CEA-852-Einheit des Geräts an. Sie wird nur angezeigt, wenn das CEA-852-Interface aktiviert ist. Der obere Teil der CEA-852-Statistikseite wird in Abbildung 44 gezeigt. Um die Statistik zu aktualisieren klicken Sie auf die Schaltfläche **Update all CEA-852 statistics**. Um alle Statistikzähler zurückzusetzen, klicken Sie auf die Schaltfläche **Clear all CEA-852 statistics**. Das Feld **Date/Time of clear** zeigt den Zeitpunkt der letzten Zählerzurücksetzung an

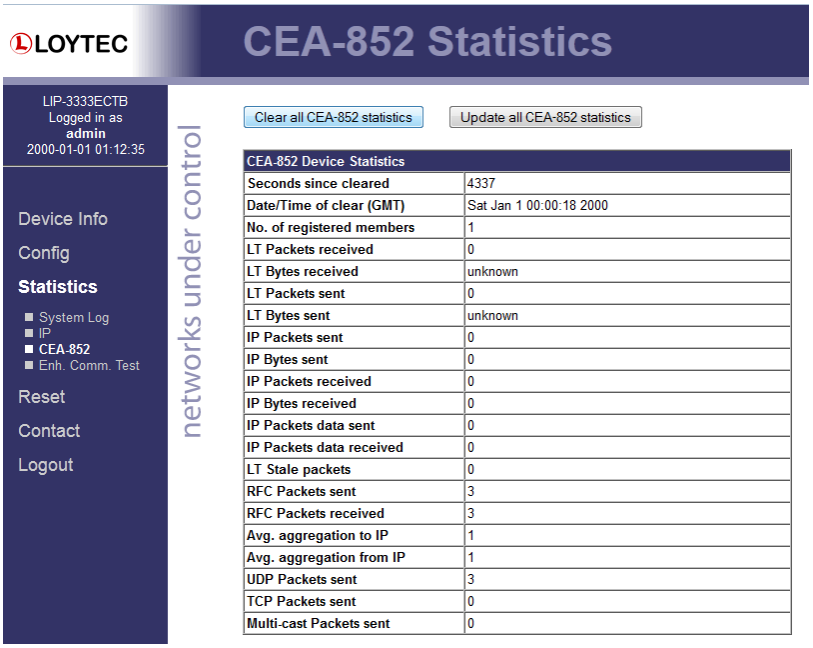


Abbildung 44: Teil der CEA-852-Statistik

7.2.4 Enhanced Communications Test

Der erweiterte Kommunikationstest erlaubt das Testen des CEA-852-Kommunikationspfades zwischen der CEA-852-Einheit des Geräts und anderen CEA-852-Geräten, sowie dem Konfigurationsserver. Die Pfade zwischen den Mitgliedern des IP-Kanals und des Konfigurationsservers werden in jede Richtung gründlich getestet. Portweiterleitungsprobleme werden erkannt. Für ältere Geräte oder Geräte anderer Hersteller, die den erweiterten Kommunikationstest nicht unterstützen, ist der Test erfolgreich, sobald das Gerät erreichbar ist. Es wird aber ein Kommentar ausgegeben, um darauf hinzuweisen, dass der Rückweg nicht getestet werden konnte. Eine typische Ausgabe ist in Abbildung 45 zu sehen.

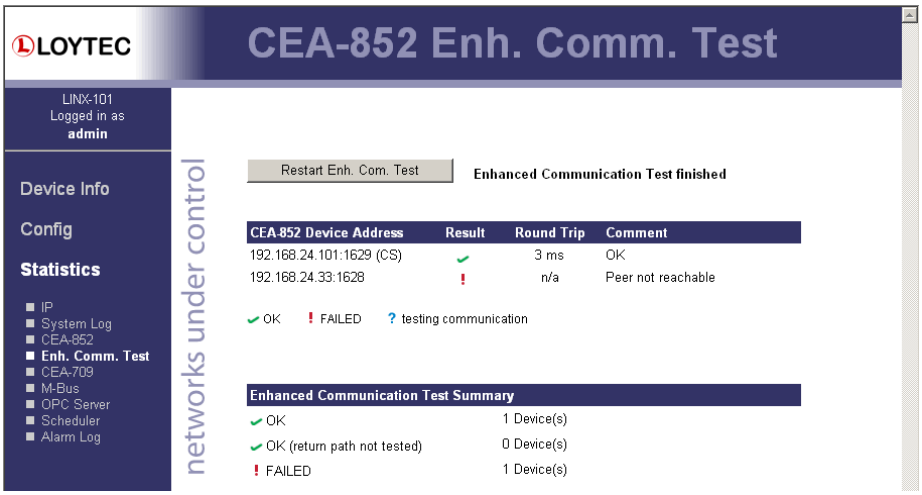


Abbildung 45: Ausgabe des erweiterten Kommunikationstests

Der Umlaufzeitwert (RTT, Round Trip Time) entspricht der gemessenen Zeit, die ein zum Zielgerät gesendetes Paket benötigt, bis es zurück zum Gerät geroutet wird. Der Umlaufzeitwert ist ein Maß für die generelle Zeitverzögerung im Netzwerk. Falls der Test eines bestimmten Mitglieds fehlschlägt, wird ein Text angezeigt, um die mögliche Ursache des Problems zu beschreiben. Die Gründe für solche Fehlschläge sind in Tabelle 4 aufgelistet.

Angezeigter Text (Web-Icon)	Bedeutung
OK, Return path not tested (OK, Rückweg nicht getestet – grüner Haken)	Wird für ein Gerät angezeigt, das erreichbar ist, aber die Anforderung, den Rückweg zu testen, nicht unterstützt (Gerät das zu diesem CEA-852 Gerät sendet). Daher kann kein potentieller NAT-Router-Konfigurationsfehler entdeckt werden. Sollte das getestete Gerät ein L-IP sein, so wird empfohlen, dieses Gerät auf Firmware 3.0 oder höher zu aktualisieren.
Not reachable/not supported (Nicht erreichbar / nicht unterstützt – rotes Rufzeichen)	Dies wird für den CS angezeigt, wenn dieser nicht erreichbar ist, oder der CS diesen Test nicht unterstützt. Um diese Unsicherheit zu eliminieren, wird empfohlen, den L-IP auf Firmware 3.0 oder höher zu aktualisieren.
Local NAT config. Error (lokaler NAT-Konfigurationsfehler – rotes Rufzeichen)	Dies wird angezeigt, wenn sich das CEA-852 Gerät hinter einem NAT-Router oder einer Firewall befindet, und die Portweiterleitung im NAT-Router (üblicherweise 1628) bzw. die Filtertabelle in der Firewall nicht korrekt ist.
Peer not reachable (Peer nicht erreichbar – rotes Rufzeichen)	Wird für nicht erreichbare Geräte angezeigt. Keine RTT wird angezeigt. Das Gerät ist entweder nicht online, nicht mit dem Netzwerk verbunden, hat keine IP-Adresse, oder ist nicht erreichbar hinter seinem NAT-Router. Führen Sie diesen Test am verdächtigen Gerät aus, um ein etwaiges NAT-Konfigurationsproblem zu entdecken.

Tabelle 4: Mögliche Kommunikationsprobleme

7.2.5 Packet Capture

Die Funktion Packet Capture erlaubt die Konfiguration und die lokale Aufzeichnung von Paketen auf dem Ethernet und MS/TP-Ports. Lesen Sie bitte den Abschnitt 14.9 für weiterführende Informationen, wie die lokale Paketaufzeichnung eingestellt und eine Remote-Aufzeichnung für Wireshark konfiguriert werden kann.

7.2.6 Mobilfunk

Auf der Seite **Mobilfunk** werden Verkehrsstatistiken über die mobile LTE-800 Mobilfunkschnittstelle angezeigt (siehe Abbildung 46). Die erste Tabelle **Datennutzung im Mobilfunknetz** enthält ein aggregiertes Daten- und SMS-Übertragungsvolumen seit dem letzten Zurücksetzen der Datennutzung. Diese Leistungsindikatoren bleiben beim Neustart des Geräts bestehen. Durch Klicken auf **Datennutzung zurücksetzen** werden diese Zähler auf 0 zurückgesetzt.

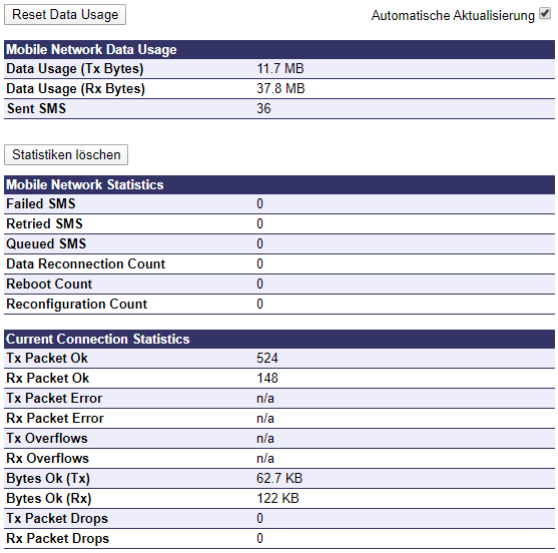


Abbildung 46: Statistikseite zum Mobilnetz.

Die zweite Tabelle **Mobile Network Statistics** enthält Informationen zu Daten und SMS-Übertragungsvolumen pro Datenverbindung. Die Schaltfläche **Statistiken löschen** löscht die

Daten dieser Tabelle, lässt jedoch das aggregierte Datenvolumen unverändert. Die dritte Tabelle enthält die Statistiken der aktuellen Datenverbindung.

7.3 Gerätekonfiguration

Die Gerätekonfigurationsseiten erlauben es, die Geräteeinstellungen anzusehen und zu ändern. Hier sind einige generelle Regeln zur Einstellung von IP-Adressen, Portnummern und Zeitwerten:

- Ein leeres IP-Adressfeld deaktiviert den Eintrag.
- Ein leeres Portnummernfeld setzt die Standardportnummer.
- Ein leeres Zeitwertfeld deaktiviert die Einstellung.

7.3.1 Systemkonfiguration

Die Systemkonfigurationsseite, wie sie in Abbildung 47 gezeigt wird, erlaubt es, die Systemzeit des Geräts und weitere Eigenschaften zu konfigurieren. Der Link **TCP/IP Configuration** ist eine Weiterleitung auf die Ethernet-Port-Konfiguration. Folgen Sie diesem Link, um die IP-Adresse des Geräts zu ändern.

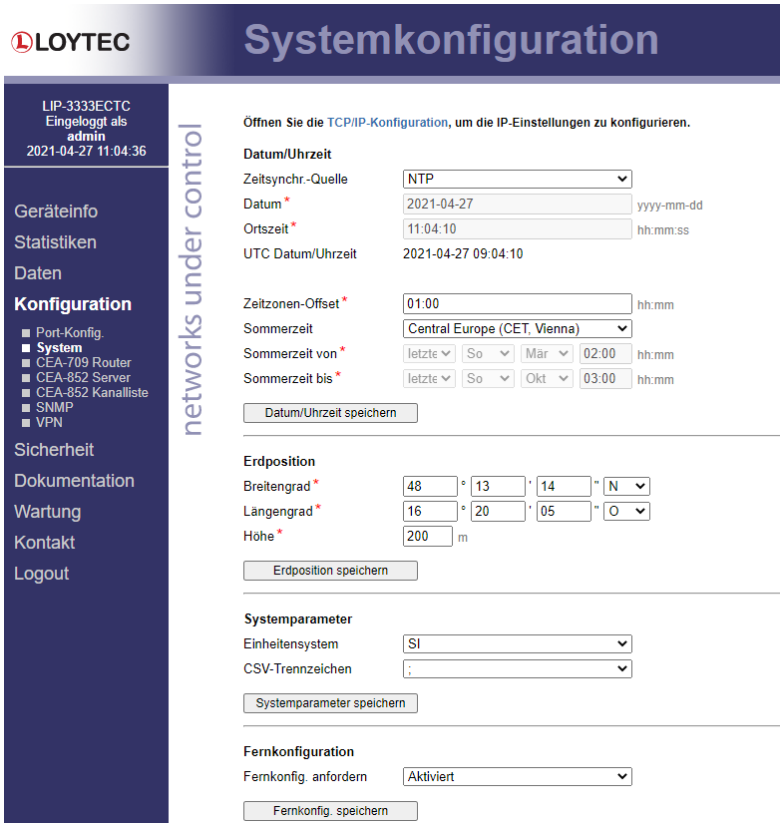


Abbildung 47: System-Konfigurationsseite, z.B. für Wien, Österreich.

Die Quelle der Zeitsynchronisation kann auf **auto**, **manual** oder **NTP** gesetzt werden. Im Modus **auto** wird das Gerät zu der ersten externen Zeitquelle, die gefunden wird, geschaltet. Die Einstellung **manual** ermöglicht das manuelle Setzen der Zeit in den Eingabefeldern **Local Time** und **Local Date**. Im Modus **manual** schaltet das Gerät nicht zu einer externen Zeitquelle. Soll **NTP** verwendet werden, so müssen die NTP Server im IP Einstellungsmenü konfiguriert sein (siehe Abschnitt 7.6.1).

Unabhängig von einer definierten Zeitquelle muss ein Offset für die Zeitzone eingestellt werden. Der Offset wird als Offset zur GMT in Stunden und Minuten angegeben (z.B. Wien/Österreich mit +1:00, New York/USA mit -6:00). Für die Einstellung der Sommerzeit stehen für Europa und USA/Kanada vordefinierte Parameter zur Verfügung. Die Sommerzeit kann jedoch auch mit **none** ausgeschaltet oder für andere Regionen manuell eingestellt werden. In diesem Fall müssen Start- und Enddatum der Sommerzeit in die darunterliegenden Felder eingegeben werden.

Im Bereich **Remote Configuration** kann eingestellt werden, ob ein Austauschgerät automatisch mit einer Konfiguration vom LWEB-900 Server bespielt werden soll.

Die Einstellung zur **Sprache** erlaubt ebenfalls die Änderung der Sprache am Web-Interface. Eine Änderung wird sofort aktiv. Diese Einstellung ist dieselbe wie auf der LCD-Anzeige.

7.3.2 Port-Konfiguration

Die Port-Konfigurationsseite erlaubt es die Kommunikationsports des Geräts zu konfigurieren. Für jeden Kommunikationsport, der auch am Gerät selbst verfügbar und dort am Label gekennzeichnet ist (z.B. Port 1, Port 2, Ethernet), existiert ein zugehöriger Karteireiter in der Web-Seite. Ein Beispiel für diese Seite ist in Abbildung 48 dargestellt. Jeder Karteireiter enthält eine Anzahl an Kommunikationsprotokollen, die auf diesem Port verfügbar sind. Durch Anhaken der jeweiligen Kontrollhäckchen bzw. Auswahlknöpfe können Protokolle auf dem Port aktiviert oder deaktiviert werden. Manche Ports erlauben nur die Auswahl eines exklusiven Protokolls. Andere Ports (z.B. Ethernet) erlauben es, gleichzeitig mehrere Protokolle zu aktivieren.

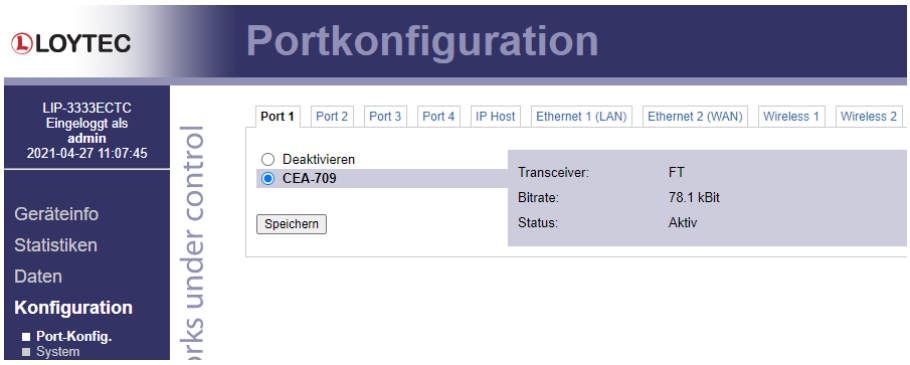


Abbildung 48: Port-Konfiguration.

Ist ein Protokoll auf einem Port angewählt, dann erscheinen rechts davon in einer Box die Protokolleinstellungen. Um die Einstellungen zu speichern, drücken Sie den Knopf **Speichern**.

7.3.3 IP-Konfiguration

Die TCP/IP-Konfiguration des Geräts erfolgt unter dem Reiter für den Ethernet-Port wie in Abbildung 49 gezeigt. Die zwingend vorgeschriebenen IP-Einstellungen, die notwendig sind, damit das Gerät richtig arbeitet, sind mit einem roten Sternchen markiert. Das **Enable DHCP**-Kontrollkästchen schaltet zwischen manueller Eingabe der IP-Adresse, Netzmasken- und Gateway-Adresse und automatischer Konfiguration durch einen DHCP-Server um.

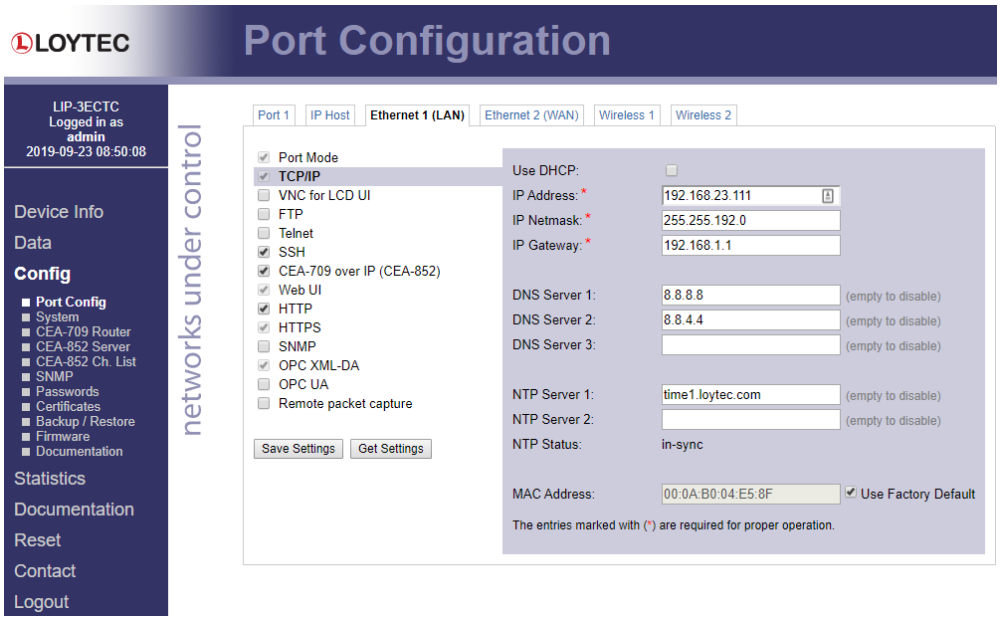


Abbildung 49: IP-Konfigurationsseite.

Das Gerät wird mit einer eindeutigen MAC-Adresse ausgeliefert. Diese Adresse kann geändert werden, um die MAC-Adresse eines anderen Geräts zu klonen. Kontaktieren Sie bitte Ihren Systemadministrator, um MAC-Adresskonflikte zu verhindern.

Die Einstellungen für DNS und NTP Servers sollten in den IP Host-Einstellungen gemacht werden (siehe Abschnitt 7.3.4). Im Falle, dass auf einem IP-Interface DHCP läuft, können hier die von DHCP zugewiesenen DNS- und NTP-Adressen eingesehen werden. Geräte mit nur einem Ethernet-Port zeigen diese Einstellungen hier nicht.

Andere Standardprotokolle, die auf dem Ethernet-Port verwendet werden, sind SSH, FTP, Telnet und HTTP (für den Web-Server). Durch Abhaken des jeweiligen Kontrollhäkchens können die einzelnen Protokolle abgeschaltet werden. Die standardmässigen UDP/TCP-Ports können in den zugehörigen Protokolleinstellungen verändert werden. Abbildung 50 zeigt zum Beispiel die Einstellungen für den SSH-Server. Beachten Sie, dass HTTP für den Web-Server nur über die LCD-Bedienung deaktiviert werden kann, oder wenn das Web-Interface über HTTPS geöffnet wurde.

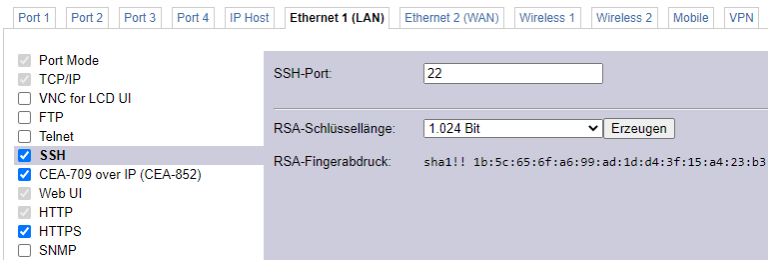


Abbildung 50: Konfiguration des SSH-Servers am Ethernet-Port.

7.3.4 Verwenden mehrerer IP-Ports

Auf Modellen mit mehreren IP-Interfaces, bietet die Port-Konfiguration einen separaten Reiter für jeden IP-Port, z.B. **Ethernet 1 (LAN)** und **Ethernet 2 (WAN)**. In der Einstellung zum Port Mode können diese Interfaces aktiviert werden, um auf einem separatem IP-Netzwerk betrieben werden zu können. Als Voreinstellung ist nur **Ethernet 1 (LAN)** aktiviert und so konfiguriert, dass es auf den Port Ethernet 2 geswitcht wird. Um **Ethernet 2 (WAN)** als ein separates, isoliertes IP-Netzwerk zu aktivieren, wählen Sie **Separate network**

in der Einstellung zum Port Mode, wie in Abbildung 51 gezeigt wird, und speichern Sie diese Einstellung. Ein Neustart ist erforderlich, damit diese Änderung wirksam wird.

Für jedes als separates Netzwerk konfigurierte IP-Interface können die einzelnen Standard-Protokolle separat aktiviert werden. In der Voreinstellung sind nur die sicheren Protokolle HTTPS, SSH und OPC UA auf einem neuen separaten IP-Interface aktiviert. Einige Protokolle können auf mehreren Interfaces gleichzeitig aktiviert werden, andere nur auf einem Interface. Wird so ein Protokoll auf einem neuen separaten IP-Interface aktiviert, erscheint eine Warnung, die anzeigt, auf welchem anderen IP-Interface dieses Protokoll infolge deaktiviert wird (z.B. bei CEA-709 over IP).

Der Modus als separates Netzwerk kann verwendet werden, wenn ein isoliertes Gebäudenetzwerk auf dem LAN betrieben werden soll und zusätzlich einige Aspekte außerhalb des Gebäudenetzwerks (als WAN bezeichnet) verfügbar sein sollen. Physikalisch werden die beiden Ethernet-Ports in unterschiedliche Ethernet-Switches verkabelt.

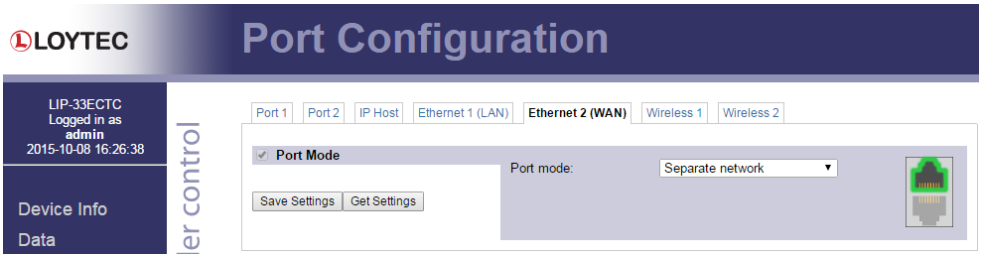


Abbildung 51: Aktivieren des Ethernet 2 (WAN) Interface.

Um ein separates IP-Interface zu deaktivieren, wählen Sie **Disable** in der Einstellung zum Port Mode. Diese Änderung wird sofort ohne Neustart wirksam. Um den geswitchten Modus wieder einzustellen, wählen Sie **Switch Ethernet 1+2** in der Einstellung zum Port Mode.

7.3.5 802.1X Port-Authentifizierung

Um die Sicherheit bei einer Netzwerkinstallation weiter zu erhöhen, verlangen IT-Abteilungen die 802.1X-Portauthentifizierungsmethode. Nach diesem Standard muss ein Gerät seinen Port am Netzwerk-Switch authentifizieren, bevor Datenverkehr in das Netzwerk zugelassen wird.

LOYTEC devices can enable 802.1X port authentication in the **Port Mode** settings on the **Ethernet** tabs of the port configuration (see Abbildung 52). Set the checkbox **Enable 802.1X**. Then choose an authentication **EAP Type** required by your IT department. The following EAP types are supported:

Auf LOYTEC-Geräten kann die 802.1X-Portauthentifizierung in der Einstellung zum Portmodus auf den Ethernet-Registerkarten der Portkonfiguration aktiviert werden (siehe Abbildung 52). Aktivieren Sie das Kontrollkästchen **802.1X aktivieren**. Wählen Sie dann einen **EAP-Typ** zur Authentifizierung aus, der von Ihrer IT-Abteilung benötigt wird. Die folgenden EAP-Typen werden unterstützt:

- **Protected EAP (PEAP)**: Definieren Sie für diesen Typ eine Methode für die innere **Authentifizierung** (z. B. MSCHAPv2) sowie **Benutzername** und **Passwort**. Die anonyme Identität und das CA-Zertifikat des Radius-Servers sind optional. Letzteres wird benötigt, wenn der Radius-Server autorisiert werden soll.

- **Tunneled TLS (TTLS)**: Definieren Sie für diesen Typ eine Methode für die innere **Authentifizierung** (z. B. PAP) sowie **Benutzername** und **Passwort**. Die Anonyme Identität und das CA-Zertifikat des Radius-Servers sind optional. Letzteres wird benötigt, wenn der Radius-Server autorisiert werden soll.

- **EAP-TLS**: Dieser Typ ist vollständig zertifikatbasiert. Es ist erforderlich, die **Identität** (Klartextname des Clients) zu definieren und ein passendes **Benutzerzertifikat** zu installieren. Dieses Zertifikat wird normalerweise vom Radius-Server ausgestellt und ist kennwortgeschützt. Um das Benutzerzertifikat hochzuladen, klicken Sie neben Benutzerzertifikat auf die Schaltfläche **Datei auswählen** und wählen Sie die Zertifikatdatei aus. Beide Zertifikatformate, PEM und PFX, werden unterstützt. Der Name wird dann angezeigt und das Kennwort für den privaten Benutzerschlüssel wird abgefragt. Geben Sie das Kennwort ein und klicken Sie auf **Speichern**, um das Zertifikat auf dem Gerät zu speichern.

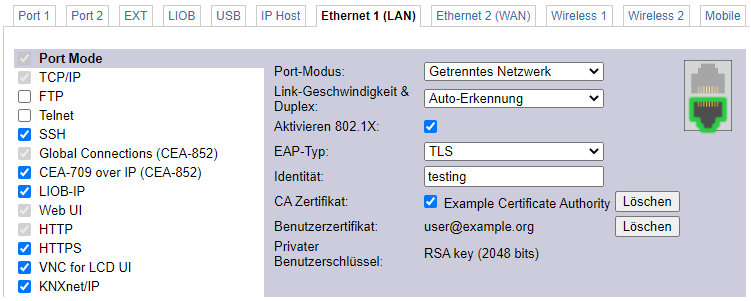


Abbildung 52: Konfiguration der 802.1X Port-Authentifizierung.

Um eines der installierten Zertifikate zu löschen, klicken Sie daneben auf die Schaltfläche **Löschen**. Anschließend kann ein anderes Zertifikat installiert werden, indem Sie auf die Schaltfläche **Datei auswählen** klicken. Die ausgewählte Datei wird neben der Schaltfläche notiert. Klicken Sie auf **Speichern**, um die ausgewählten Zertifikate am Gerät zu speichern.

7.3.6 IP Host-Konfiguration

Auf den L-IP Modellen, , die über einen eingebauten Ethernet Switch/Hub verfügen, gibt es einen eigenen Reiter IP Host, auf dem die gemeinsamen Host-Einstellungen bearbeitet werden können, wie in Abbildung 53 gezeigt. Diese Einstellungen betreffen alle IP-Interfaces auf dem Gerät. Auf Modellen mit einem einzelnen Ethernet-Port befinden sich die IP Host-Einstellungen direkt am Ethernet-Reiter.

Hostname und **Domainname** sind optionale Einträge und können leer gelassen werden. Bei manchen DHCP-Konfigurationen kann es notwendig sein, einen Hostnamen anzugeben. Bitte kontaktieren Sie Ihren Systemadministrator um zu erfahren, wie Sie eine korrekte Konfiguration via DHCP vornehmen können, um eine IP-Adresse zu erhalten.

Die Einstellung **Default Gateway** legt das Gateway von einem bestimmten IP-Interface fest, auf das aller nicht lokaler Netzwerkverkehr geleitet wird. Dazu muss eines der vorhandenen IP Interfaces mit separatem Netzwerk ausgewählt werden.

Weiters können bis zu drei DNS Server auf dieser Seite konfiguriert werden. Diese DNS Server werden von allen Diensten auf allen IP-Interfaces zur Namensauflösung kontaktiert. Für den Fall, dass DNS Server auf einem Interface über DHCP eingestellt werden, ändern Sie die Einstellung **Use DNS servers from** so, dass sie auf dieses Interface verweist.

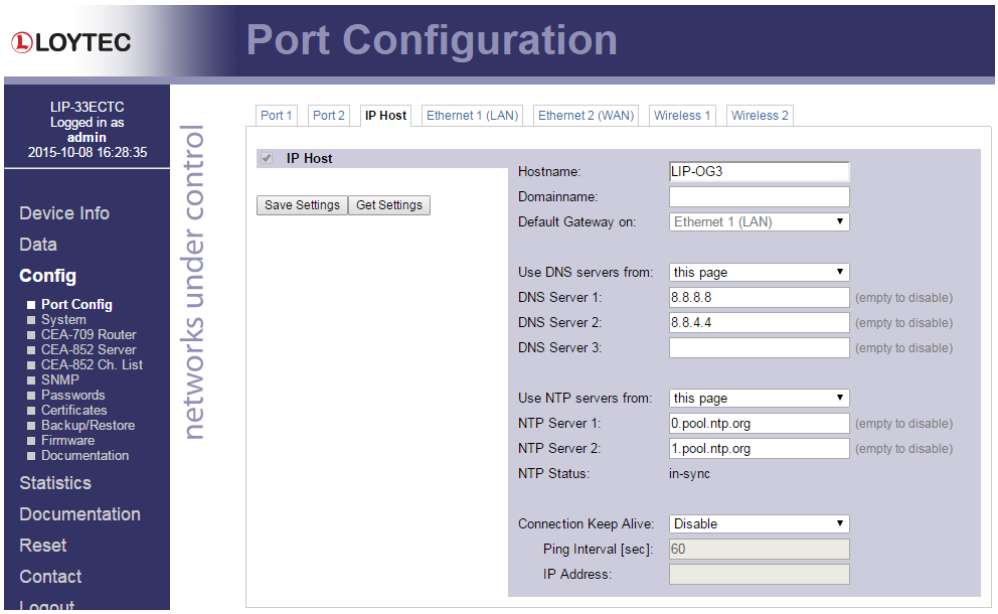


Abbildung 53: Einstellungen auf dem Reiter für IP Host.

Das Gerät kann so konfiguriert werden, dass die Systemzeit per NTP synchronisiert wird. Geben Sie in den entsprechenden Feldern die Adresse des primären und optional des sekundären NTP-Servers ein. Ist in der Systemkonfiguration **NTP** als Zeitsynchronisationsquelle eingestellt (siehe Abschnitt 7.3.1) wird NTP zur Synchronisation herangezogen. Im Feld **NTP status** unterhalb der „NTP Server"-Einstellungen wird der aktuelle Status der NTP Synchronisation angezeigt (**out-of-sync** oder **in-sync**). Die Einstellungen, die hier gemacht werden, wirken auf alle IP-Interfaces. Für den Fall, dass NTP Server auf einem Interface über DHCP eingestellt werden, ändern Sie die Einstellung **Use NTP servers from** so, dass sie auf dieses Interface verweist.

Die Funktion **Connection Keep Alive** erlaubt es, automatisch andere Geräte auf dem IP-Netzwerk zu pingen, um eine IP-Verbindung aufrecht zu erhalten, die sonst nach einer bestimmten Zeit abgebrochen werden würde (z.B. könnte ein DSL-Router ohne Aktivität automatisch die Verbindung lösen). Zum Aktivieren wählen Sie eine der beiden Optionen Auto IP oder Custom IP.

Wenn der Auto-IP Modus gewählt wurde und das Gerät als CEA-852 Configuration Server agiert, sendet er Ping-Nachrichten an alle CEA-852 Geräte in der Kanalliste des Configuration Servers. Ist der Configuration Server auf dem Gerät abgeschaltet, wird eine Ping-Nachricht an den Configuration Server des IP-852 Kanals gesendet. Wurde Custom IP gewählt, kann eine bestimmte IP-Adresse eingegeben werden, die gepingt werden soll.

7.3.7 Dynamic DNS Konfiguration

LOYTEC-Geräte können so konfiguriert werden, dass sie sich für einen dynamischen DNS-Dienst registrieren. Die Einstellungen werden im Detailbereich für das Protokoll **Dynamic DNS** auf der Registerkarte **IP Host** der Portkonfiguration vorgenommen (siehe Abbildung 12). Wählen Sie den **Provider** aus, bei dem Ihr Domainname registriert wurde, und geben Sie die anbieterspezifischen Details in die folgenden Felder ein. In der Regel umfasst dies den registrierten **Domainnamen** oder die URL sowie ein Kennwort oder ein Sicherheits-Token.

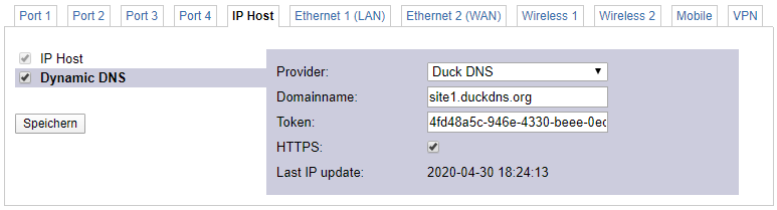


Abbildung 54: Dynamic DNS Einstellungen

7.3.8 WLAN-Konfiguration

Geräte mit USB-Anschluss, welche den LWLAN-800 WLAN-Adapter unterstützen, können in IEEE 802.11 Drahtlosnetzwerke eingebunden werden. Die grundlegenden Funktionen zum Betrieb im WLAN werden in Abschnitt 12.5 beschrieben. Abhängig von der gewünschten Wireless-Betriebsart, wählen Sie den Reiter **WLAN Client** oder **WLAN Access Point** der Port-Konfiguration. Als ersten Schritt zur Konfiguration aktivieren die Das Protokoll **Wireless** am jeweligen Reiter, wie in Abbildung 55 gezeigt ist.

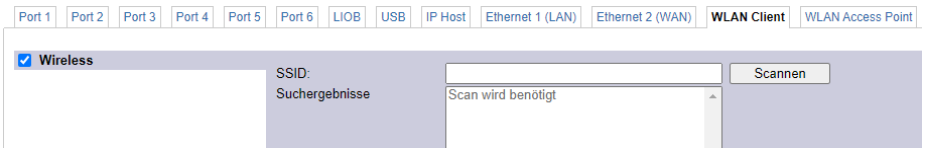


Abbildung 55: Wireless Port Mode

WLAN Client Reiter: Auf dieser Registerkarte können Sie die WLAN-Schnittstelle im Client-Modus konfigurieren. In diesem Modus verbindet sich der WLAN-Client mit einem bestehenden Access Point. Abbildung 56 zeigt die Einstellungen des WLAN-Interfaces im Client-Modus.

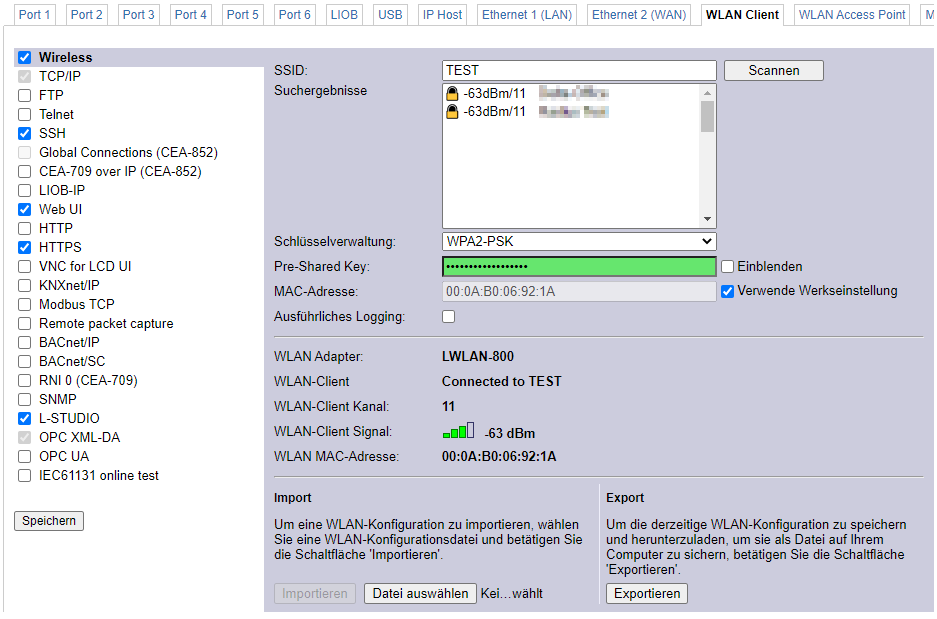


Abbildung 56: WLAN-Client Einstellungen

Die folgenden Einstellungen werden im Client-Modus benötigt:

- **SSID**: Die Service-Set-ID identifiziert das Drahtlosnetzwerk zu dem sich das Gerät verbinden soll. Es kann manuell eingegeben werden, wenn beispielsweise die SSID nicht ausgesendet wird. Mit dem Knopf **scan** kann nach verfügbaren WLAN-Netzwerken gesucht werden. Beachten Sie, dass das Scannen den normalen Betrieb

einer bestehenden Verbindung unterbricht. Daher sollte der Scan-Vorgang nur beim Setup ausgelöst werden.

- **Suchergebnisse**: Diese Liste zeigt die gefundenen WLAN-Netzwerke und ihre Signalstärke an. Durch Auswählen eines Eintrags der Liste wird er im SSID-Feld übernommen.

- **Schlüsselverwaltung**: Dieses Feld wählt die Verschlüsselungsverwaltung aus. Zur Auswahl stehen NONE (unverschlüsselt), WEP, WPA und WPA2. Die empfohlene Auswahl ist WPA2, da WPA und WEP heute aus unsicher betrachtet werden müssen. Sie stehen aus Kompatibilitätsgründen weiter zur Auswahl.

- **Pre-Shared Key**: Dieses Feld legt das Passwort für das WLAN-Netzwerk fest. Durch Setzen des Hakens **show** wird das Passwort im Klartext angezeigt.

- **Ausführliches Logging**: Für den Fall, dass Kommunikationsprobleme auftreten, können ausführliche Informationen in das OS-Log geschrieben werden. Es wird empfohlen, diese Option nicht im Normalbetrieb zu verwenden.

Auf der Seite werden die folgenden Informationen angezeigt:

- **WLAN-Adapter**: Typ des angeschlossenen WLAN-Adapters.

- **WLAN Client**: Zeigt an, ob das Interface zu einem Netzwerk verbunden ist.

- **WLAN Client Kanal**: Zeigt den Wireless-Kanal an.

- **WLAN Client Signal**: Die Signalstärke des WLAN-Signals.

- **WLAN MAC-Adresse**: MAC-Adresse des WLAN-Adapters.

WLAN Access Point Reiter: Auf dieser Registerkarte können Sie einen WLAN Access Point oder einen Mesh Point konfigurieren, indem Sie aus der Dropdown-Liste **Wireless-Modus** auswählen:

- Access Point: Das Gerät bietet einen eigenen WLAN Access Point, wohin sich andere Clients ins Wireless-Netzwerk des Geräts verbinden können.

- Mesh Point: In diesem Modus wird ein Mesh-Netzwerk nach IEEE 802.11s aufgebaut (siehe Abschnitt 7.3.9).

Die Einstellungen des Access-Point-Modus sind in Abbildung 57 gezeigt.

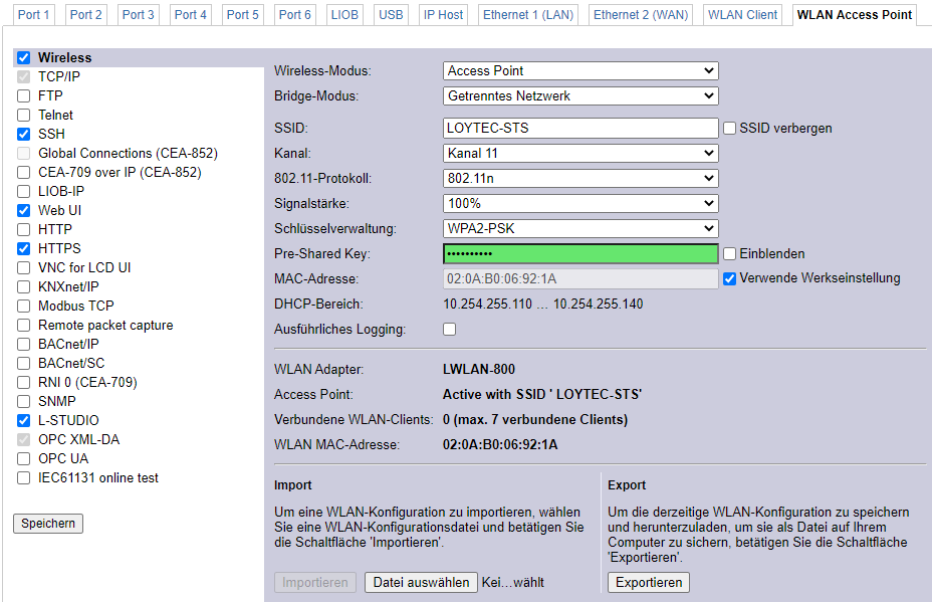


Abbildung 57: Einstellungen als WLAN Access Point.

Die folgenden Einstellungen konfigurieren den Access-Point:

- **Bridge-Modus**: Der Access Point kann entweder als separates Netzwerk oder zu Ethernet 1 als Brücke betrieben werden. Nach der Konfiguration des Access Points müssen die TCP/IP-Einstellungen für das WLAN-Interface konfiguriert werden, wenn der Port als separates Netzwerk eingestellt wurde. Diese werden wie für ein Ethernet-Interface konfiguriert (siehe auch Abschnitt 7.3.4). Für einen Access Point im separaten Netzwerkmodus werden die IP-Adresse und die Netzmaske verwendet, um das Netzwerk zu definieren, in dem der Client eine IP-Adresse vom integrierten DHCP-Server erhält. DNS- und NTP-Einstellungen sind in diesem Modus nicht erforderlich.

- **SSID**: In diesem Feld wird die Service-Set-ID eingestellt, die das WLAN-Netzwerk identifiziert. Das Setzen des Hakens **hide SSID** verhindert das Aussenden der SSID, sodass dieses Netzwerk beim Scannen nicht gefunden wird. Beachten Sie bitte, dass das Verbergen mehr Sicherheitsimplikationen als das Aussenden hat, wodurch diese Option deaktiviert bleiben sollte.

- **Kanal**: Dieses Feld wählt den Funkkanal aus. Im 2,4GHz-Band gibt es 13 Kanäle. Allerdings überlappen sich diese, wodurch nicht alle Kanäle interferenzfrei verwendet werden können. Wenn möglich, verwenden Sie die Kanäle 1, 6 und 11, um überlappende Funkbänder zu vermeiden.

- **802.11 Protokoll**: Dieses Feld wählt das Funkprotokoll des Access-Points aus. Die empfohlene Standardeinstellung 802.11b/g/n unterstützt alle Protokolle. Sollten einige Clients Kompatibilitätsprobleme haben, kann der Access-Point auf 802.11b/g oder 802.11b eingeschränkt werden.

- **Signalstärke**: Dieses Feld wählt die Sendesignalstärke zwischen 5 und 100%. Diese kann verringert werden, wenn die Interferenz mit weiter entfernten Knoten minimiert werden soll. Üblicherweise kann die Voreinstellung von 100% belassen werden.

- **Schlüsselverwaltung**: Dieses Feld definiert die Schlüsselverwaltung. Zur Auswahl stehen NONE (unverschlüsselt), WEP, WPA und WPA2. Die empfohlene Auswahl ist WPA2, da WPA und WEP heute als unsicher betrachtet werden müssen. Sie stehen aus Kompatibilitätsgründen weiter zur Auswahl.

- **Pre-Shared Key**: Dieses Feld legt das Passwort für das WLAN-Netzwerk fest. Durch Setzen des Hakens **show** wird das Passwort im Klartext angezeigt.

- **Ausführliches Logging**: Für den Fall, dass Kommunikationsprobleme auftreten, können ausführliche Informationen in das OS-Log geschrieben werden. Es wird empfohlen, diese Option nicht im Normalbetrieb zu verwenden.

Auf der Seite werden die folgenden Informationen angezeigt:

- **WLAN-Adapter**: Typ des angeschlossenen WLAN-Adapters.

- **WLAN Access-Point**: Zeigt den Status des Access-Point an.

- **Verbundene WLAN Clients**: Zeigt die Anzahl an verbundenen WLAN-Clients an.

- **WLAN MAC-Address**: MAC-Adresse des WLAN-Adapters.

Mit den Schaltflächen im unteren Bereich können Sie die WLAN-Konfiguration exportieren und importieren. Damit ist es möglich, ein Gerät zu konfigurieren und die Konfiguration auf andere Geräte zu übertragen. Der **Export** -Knopf speichert die Konfiguration in eine Datei am PC ab. Der **Import**-Knopf importiert die Konfiguration. Nachdem Sie die WLAN-Einstellungen geändert haben, müssen Sie auf **Speichern** klicken und das Gerät neu starten, damit die Einstellungen aktiv werden.

Achtung: *Der LWLAN-800 unterstützt insgesamt maximal 7 verbundene Clients.*

7.3.9 Mesh-Konfiguration

Geräte mit USB-Anschluss, welche den LWLAN-800 WLAN-Adapter unterstützen oder Geräte mit integriertem WLAN-Adapter, können ein Mesh-Netzwerk nach dem IEEE Standard 802.11s aufbauen. Die grundlegenden Funktionen zum Betrieb eines Mesh-Netzwerkes werden in Abschnitt 12.5.2 näher beschrieben. Das Mesh-Netzwerk wird auf der Karteikarte **WLAN Access Point** konfiguriert. Die Einstellungen für **Bridge Modus** und **TCP/IP** in der Port-Konfiguration werden für das Mesh-Netzwerk auf dieselbe Art konfiguriert, wie im Abschnitt 7.3.8 für den Access Point beschrieben. Die Konfigurations-einstellungen für den Mesh-Point oder Mesh-Portal Modus werden in Abbildung 58 gezeigt.

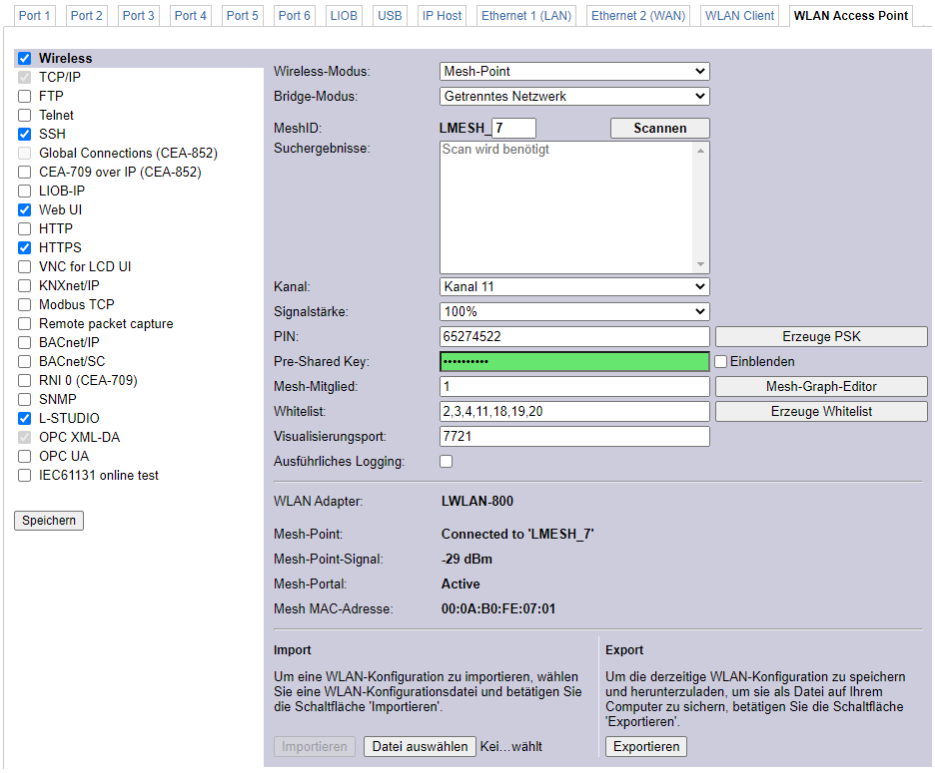


Abbildung 58: WLAN Mesh Netzwerkeinstellungen

Die folgenden Einstellungen konfigurieren den Mesh-Point:

- **Wireless-Modus**: Wählen Sie **Mesh Point**, um die Schnittstelle als Mesh Point zu konfigurieren.

- **Bridge-Modus**: Der Mesh Point kann entweder als separates Netzwerk oder zu Ethernet 1 als Brücke betrieben werden. Nach der Konfiguration des Mesh Point müssen die TCP/IP-Einstellungen für das WLAN-Interface konfiguriert werden, wenn der Port als separates Netzwerk eingestellt wurde. Diese werden wie für ein Ethernet-Interface konfiguriert (siehe auch Abschnitt 7.3.4).

- **MeshID**: Die Mesh-ID identifiziert das Drahtlosnetzwerk zu dem sich das Gerät verbinden soll. Es kann manuell eingegeben werden oder mit dem Knopf **scan** nach verfügbaren Mesh-Netzwerken gesucht werden. Beachten Sie, das Scannen den normalen Betrieb einer bestehenden Verbindung einschränkt. Daher sollte der Scan-Vorgang nur beim Setup ausgelöst werden. Ein zulässiger Wert für eine Mesh-ID liegt zwischen 1 und 255.

- **Suchergebnisse**: Diese Liste zeigt die gefundenen Mesh-Netzwerke, die verwendeten Funkkanäle und ihre Signalstärke an. Durch Auswählen eines Eintrags der Liste werden die Mesh-ID und der zugehörige Funkkanal übernommen.

- **Kanal**: Dieses Feld wählt den Funkkanal aus. Im 2,4GHz-Band gibt es 11 Kanäle. Allerdings überlappen sich diese, wodurch nicht alle Kanäle interferenzfrei verwendet werden können. Wenn möglich, verwenden Sie die Kanäle 1, 6 und 11, um überlappende Funkbänder zu vermeiden. In einem Mesh-Netzwerk müssen alle Teilnehmer denselben Kanal verwenden.

- **Signalstärke**: Dieses Feld wählt die Sendesignalstärke des Mesh-Netzwerks zwischen 5 und 100%. Diese kann verringert werden, wenn die Interferenz mit weiter entfernten Knoten minimiert werden soll. Üblicherweise kann die Voreinstellung von 100% belassen werden.

- **PIN**: In diesem Feld kann ein bis zu 8-stelliger PIN eingegeben werden, der über den Knopf **Generate PSK** einen 64-stelligen Pre-Shared Key erzeugt. Der PIN dient außerdem zur einfacheren Mesh-Konfiguration über das LCD Display.

- **Pre-Shared Key**: Dieses Feld legt das Passwort für das Mesh-Netzwerk fest. Durch Setzen des Hakens **show** wird das Passwort im Klartext angezeigt.

- **Mesh-Mitglied**: Über dieses Feld wird die Mesh-Teilnehmernummer konfiguriert. Diese muss pro MeshID eindeutig sein. Über den Knopf **Erzeuge Whitelist** kann eine Default-Whitelist generiert werden. Ein zulässiger Wert für eine Mesh-Teilnehmernummer liegt zwischen 1 und 20.

- **Whitelist**: Dieses Feld erlaubt die Konfiguration von maximal 7 Mesh-Teilnehmernummern. Den hier angeführten Mesh-Teilnehmern wird erlaubt, eine Verbindung mit diesem Mesh-Point einzugehen. Über den Knopf **Mesh Graph Editor** wird der grafische Editor zur vereinfachten Konfiguration der Whitelisten im Mesh-Netzwerk geöffnet.

Achtung: ***Der LWLAN-800 unterstützt insgesamt maximal 7 verbundene Clients.***

- **Visualisierungsport**: In diesem Feld kann der UDP-Port zur Mesh-Netzwerkvisualiserung festgelegt werden. Durch eine Konfiguration des UDP-Ports mit 0 wird die Mesh-Netzwerkvisulisierung auf diesem Gerät deaktiviert.

- **Ausführliches Logging**: Für den Fall, dass Kommunikationsprobleme auftreten, können ausführliche Informationen in das OS-Log geschrieben werden. Es wird empfohlen, diese Option nicht im Normalbetrieb zu verwenden.

Unter den Einstellungen werden auf der Seite die folgenden Informationen angezeigt:

- **WLAN-Adapter**: Typ des angeschlossenen WLAN-Adapters.

- **Mesh Point**: Zeigt an, ob das Interface zu einem Netzwerk verbunden ist.

- **Mesh Point Signal**: Zeigt die Feldstärke der Funkverbindung an.

- **Mesh Portal**: Zeigt an, ob der Mesh-Point als Mesh-Portal konfiguriert ist.

- **Mesh MAC-Address**: MAC-Adresse des WLAN-Adapters.

Die Knöpfe im unteren Bereich exportieren und importieren WLAN-Konfigurationen. Damit ist es möglich, ein Gerät zu konfigurieren und die Konfiguration auf andere Geräte zu übertragen. Der **Export**-Knopf speichert die Konfiguration in eine Datei am PC ab. Der **Import**-Knopf importiert die Konfiguration, nachdem sie mit dem **Browse**-Knopf ausgewählt wurde. Nach dem Einstellen der WLAN-Optionen, muss die Konfiguration mit **Save Settings** gespeichert und ein Neustart durchgeführt werden.

Mesh Graph Editor. Die grafische Unterstützung zur vereinfachten Konfiguration der Whitelisten im Mesh-Netzwerk wird in Abbildung 59 und Abbildung 60 dargestellt. Je nach Konfiguration der Mesh-Points und Verbindungen im Mesh-Graphen, werden die Whitelisten für die im Mesh-Graphen vorhandenen Mesh-Points dargestellt. Bei Änderungen im Mesh Graphen werden diese aktualisiert. Die folgenden Operationen sind verfügbar:

- Mesh-Point hinzufügen: Mit einem einfachen Klick in den freien Raum des Graph Editors wird ein Mesh-Point mit der im Mesh Graphen niedriegsten freien Mesh-Teilnehmernummer angelegt. Bis zu 20 Mesh-Points können im Mesh Graphen angelegt werden.

- Verbindung hinzufügen: Durch einfaches Ziehen von einem Knoten zu einem anderen beliebigen Knoten, wird eine Verbindung gezeichnet, die einen Eintrag der Mesh-Teilnehmernummer in den jeweiligen Whitelisten repräsentiert. Um das Limit der maximalen Mesh-Teilnehmer in einer Whitelist nicht zu überschreiten, sind nur 7 Verbindungen an einem Mesh-Point möglich.

- Mesh-Point/Verbindung löschen: Wählen Sie einen Mesh-Point oder eine Verbindung durch einfaches klicken aus und drücken Sie die Entfernen-Taste. Durch Drücken der ESC-Taste wird die Markierung wieder aufgehoben.

- Mesh-Teilnehmernummer ändern: Führen Sie einen Doppelklick auf einen Mesh-Point aus und geben Sie eine neue Mesh-Teilnehmernummer an.

- Graph Layout ändern: Mit gehaltener Strg-Taste können Mesh-Points beliebig im Mesh Graphen verschoben werden, um das Layout an die tatsächlichen Gegebenheiten anzupassen.

- Grundrissplan hinzufügen: Über den Knopf **Load Floorplan** kann ein als .jpg oder .png gespeicherter Grundrissplan geladen werden. Mit gehaltener Strg-Taste und dem Klicken auf den Hintergrund kann der dargestellte Grundrissplan beliebig angepasst werden.

- Grundrissplan skalieren: Über die Auswahlbox unterhalb des Grundrissplans kann der Skalierungsfaktor ausgewählt werden.

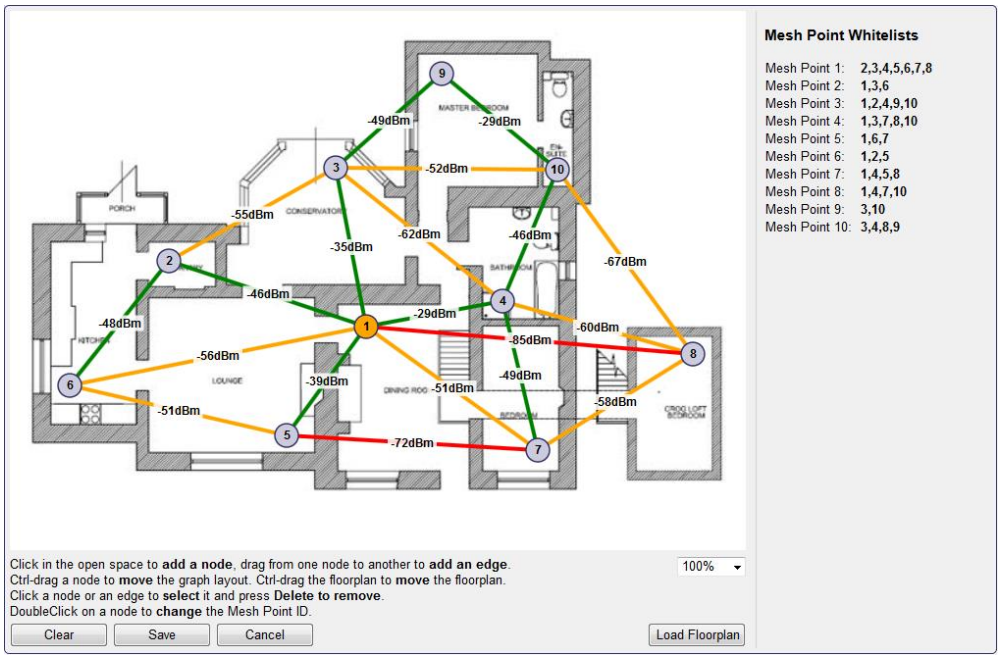


Abbildung 59: Mesh Grundrissplan in der Draufsicht und Online Link-Monitor

Durch die Verwendung eines Grundrissplans im Mesh-Graphen können bei der Konfiguration des Mesh-Netzwerks die räumlichen Gegebenheiten etwas berücksichtigt werden. Abbildung 59 zeigt einen Screenshot der Mesh-Netzwerkvisualisierung mit einem Übersichtsplan einer Gebäudeebene in der Draufsicht. Im Gegensatz dazu wird in Abbildung 60 ein Screenshot mit einem Übersichtsplan eines Gebäudes mit fünf Stockwerken in der Seitenansicht dargestellt. Ist die Mesh-Netzwerkaktualisierung über UDP aktiviert, wird auf den Verbindungen in Echtzeit die aktuelle Signalstärke zwischen den Mesh-Teilnehmern angezeigt. Die Verbindungen werden abhängig von der Signalstärke farblich hinterlegt. Grün steht für eine gute Verbindung über -50 dBm, orange für eine ausreichende Verbindung von -50 dBm bis -70 dBm und rot für eine schwache Verbindung unter -70 dBm. Anhand der

farblichen Hinterlegung ist es relativ einfach schwache Verbindungen ausfindig zu machen und Schwachstellen in der Konfiguration zu beheben.

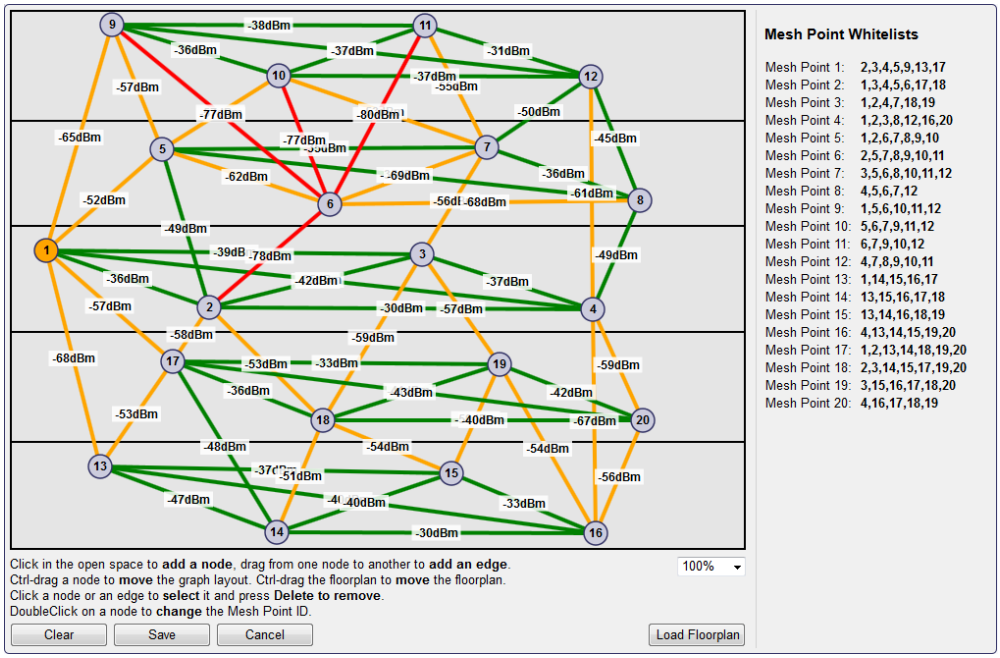
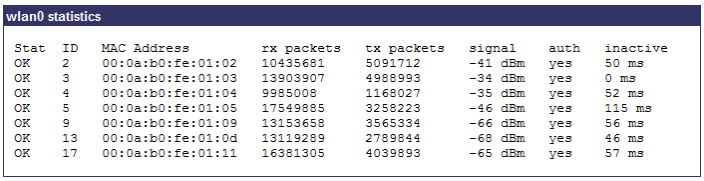


Abbildung 60: Mesh Grundrissplan in der Seitenansicht und Online Link-Monitor

Mesh-Knotenstatistik. Eine schlechte Performance oder Zuverlässigkeit eines Mesh-Netzwerks kann mehrere Gründe haben. Einer davon ist ein schlecht in das Mesh-Netzwerk integrierter Mesh-Knoten. Dieser zeigt sich im Mesh-Netzwerk meist mit einer schlechten Verbindung zu anderen Mesh-Knoten. Abbildung 61 zeigt die Mesh-Knotentatistik mit den direkt verbundenen Mesh-Knoten. Diese Statistik bietet Informationen über die Mesh-Knoten ID, die MAC-Adresse, die empfangenen bzw. gesendeten Datenpakete, die Signalstärke, den Status der Authentifizierung und die Zeit der Inaktivität.



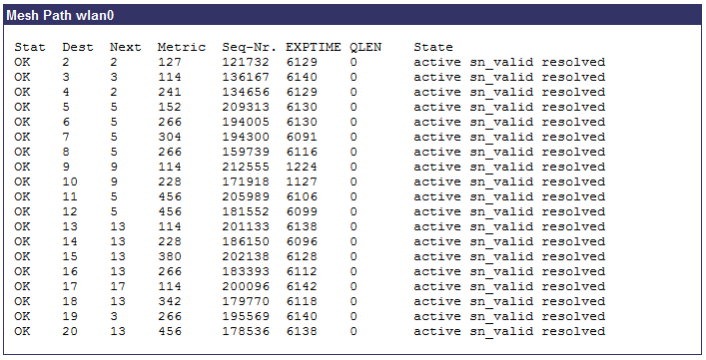
wlan0 statistics

Stat	ID	MAC Address	rx packets	tx packets	signal	auth	inactive
OK	2	00:0a:b0:fe:01:02	10435681	5091712	-41 dBm	yes	50 ms
OK	3	00:0a:b0:fe:01:03	13903907	4988993	-34 dBm	yes	0 ms
OK	4	00:0a:b0:fe:01:04	9985008	1168027	-35 dBm	yes	52 ms
OK	5	00:0a:b0:fe:01:05	17549885	3258223	-46 dBm	yes	115 ms
OK	9	00:0a:b0:fe:01:09	13153658	3565334	-66 dBm	yes	56 ms
OK	13	00:0a:b0:fe:01:0d	13119289	2789844	-68 dBm	yes	46 ms
OK	17	00:0a:b0:fe:01:11	16381305	4039893	-65 dBm	yes	57 ms

Abbildung 61: Mesh-Knotenstatistik

Wichtige Statistikwerte hierbei sind die Signalstärke und der Status der Authentifizierung. Die Statusinformation der Authentifizierung sollte beim Betrieb des Mesh-Netzwerks stets eine durchgeführte Authentifizierung signalisieren und die Signalstärke sollte für eine ausreichend gute Verbindung nicht unter -70 dBm fallen.

Mesh-Pfadstatistik. Die in Abbildung 62 dargestellte Mesh-Pfadstatistik gibt Auskunft über die Mesh-Pfade zu allen Mesh-Knoten im Mesh-Netzwerk. Jeder Mesh-Pfad ist in der Statistik mit der Empfänger Mesh-Knoten ID angeführt. Weiters wird für den jeweiligen Mesh-Pfad die Mesh-Knoten ID des Nachbars-Knoten angeführt, zu dem Datenpakete weitergeleitet werden, die an den Empfänger Mesh-Knoten adressiert sind. Weitere Statistikinformationen sind die Mesh-Pfad Metrik, die Sequenznummer, die Gültigkeitsdauer, die zwischengespeicherten Pakete und der Status des Mesh-Pfades.



Mesh Path wlan0

Stat	Dest	Next	Metric	Seq-Nr.	EXPTIME	QLEN	State
OK	2	2	127	121732	6129	0	active sn_valid resolved
OK	3	3	114	136167	6140	0	active sn_valid resolved
OK	4	2	241	134656	6129	0	active sn_valid resolved
OK	5	5	152	209313	6130	0	active sn_valid resolved
OK	6	5	266	194005	6130	0	active sn_valid resolved
OK	7	5	304	194300	6091	0	active sn_valid resolved
OK	8	5	266	159739	6116	0	active sn_valid resolved
OK	9	9	114	212555	1224	0	active sn_valid resolved
OK	10	9	228	171918	1127	0	active sn_valid resolved
OK	11	5	456	205989	6106	0	active sn_valid resolved
OK	12	5	456	181552	6099	0	active sn_valid resolved
OK	13	13	114	201133	6138	0	active sn_valid resolved
OK	14	13	228	186150	6096	0	active sn_valid resolved
OK	15	13	380	202138	6128	0	active sn_valid resolved
OK	16	13	266	183393	6112	0	active sn_valid resolved
OK	17	17	114	200096	6142	0	active sn_valid resolved
OK	18	13	342	179770	6118	0	active sn_valid resolved
OK	19	3	266	195569	6140	0	active sn_valid resolved
OK	20	13	456	178536	6138	0	active sn_valid resolved

Abbildung 62: Mesh-Pfadstatistik

Die wichtigsten Informationen der Mesh-Pfadstatistik sind die Mesh-Pfad Metrik und der Status des Mesh-Pfades. Die Mesh-Pfad Metrik gibt den Wert der Pfadqualität von diesem Mesh-Knoten zum Empfänger Mesh-Knoten wieder. Umso kleiner die Mesh-Pfad Metrik ist, desto besser ist die Verbindung zu dem Empfänger Mesh-Knoten. Ein Wert größer als 500 sollte jedoch nicht erreicht werden. In diesem Fall sollte die Mesh-Knoten Whitelist für diesen Mesh-Pfad optimiert werden. Der Status des Mesh-Pfades sollte beim Betrieb des Mesh-Netzwerks stets active, sn_valid und resolved anzeigen. Dies bedeutet einen aktiven, aufgelösten Mesh-Pfad mit einer gültigen Sequenznummer.

7.3.10 VNC-Konfiguration

LOYTEC-Geräte, die mit einer LCD-Anzeige ausgestattet sind, bieten auch entfernten Zugriff auf diese Anzeige über Ethernet. Dafür wird das VNC-Protokoll verwendet und das Gerät implementiert einen VNC-Server, um die Anzeige anzubieten. Der VNC-Server am Gerät ist standardmäßig nicht aktiviert. Am PC muss dazu nur ein VNC-Client installiert werden. Mit den Standardeinstellungen verbindet man sich auf den Port 5900 des Geräts. Das Passwort ist ‘loytec4u’.

Der VNC-Server kann über den **Ethernet**-Karteireiter der Portkonfiguration aktiviert werden. Um den VNC-Server einzuschalten, aktivieren Sie den Eintrag **VNC for LCD UI**. Die Einstellungen für das VNC-Protokoll werden in dem Kasten rechts angezeigt (siehe Abbildung 63). Der **VNC port** und das **VNC password** können hier geändert werden. In der Standardeinstellung kann sich nur ein VNC-Client mit dem Gerät verbinden. Diese Limitierung kann durch **Max VNC clients** angepasst werden. Um Änderungen über das LCD-Display mittels VNC durch einen PIN-Code zu schützen, kann ein **Admin PIN code** konfiguriert werden. Um den Schutz zu entfernen, geben Sie ‚0000’ ein.

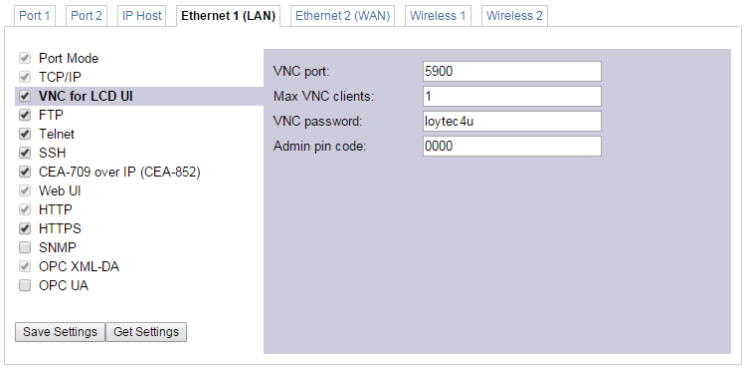


Abbildung 63: VNC-Konfiguration.

7.3.11 CEA-709-Konfiguration

Das CEA-709-Protokoll kann auf den Ports Port 1, Port 2, usw. auf dem Gerät aktiviert werden. Um das CEA-709-Protokoll zu aktivieren, drücken Sie den Auswahlknopf

CEA-709, wie in Abbildung 64 dargestellt. Beachten Sie, dass abhängig vom Modell des Geräts in diesem Fall andere Protokolle am selben Port deaktiviert werden. Informationen über die aktuellen Transceivereinstellungen werden in dem Kasten rechts angezeigt.

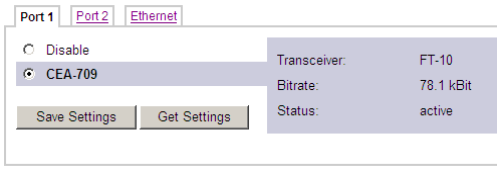


Abbildung 64: CEA-709-Konfiguration.

7.3.12 CEA-852-Gerätekonfiguration

Das CEA-852-Protokoll ist nur auf dem Ethernet-Port verfügbar. Um CEA-852 auf dem Gerät zu aktivieren, wählen Sie das Kontrollhäkchen **CEA-709 over IP (CEA-852)** auf dem **Ethernet**-Karteireiter der Port-Konfigurationsseite.

Die Einstellungen zum CEA-852-Protokoll werden in der Box rechts dargestellt, wie in Abbildung 65 gezeigt wird. Das CEA-852-Gerät wird einem IP-Kanal typischerweise durch Eingabe der relevanten Informationen auf einem Konfigurationsserver hinzugefügt. Der Konfigurationsserver kontaktiert dann die CEA-852-Einheit des L-IP und sendet seine Konfiguration.

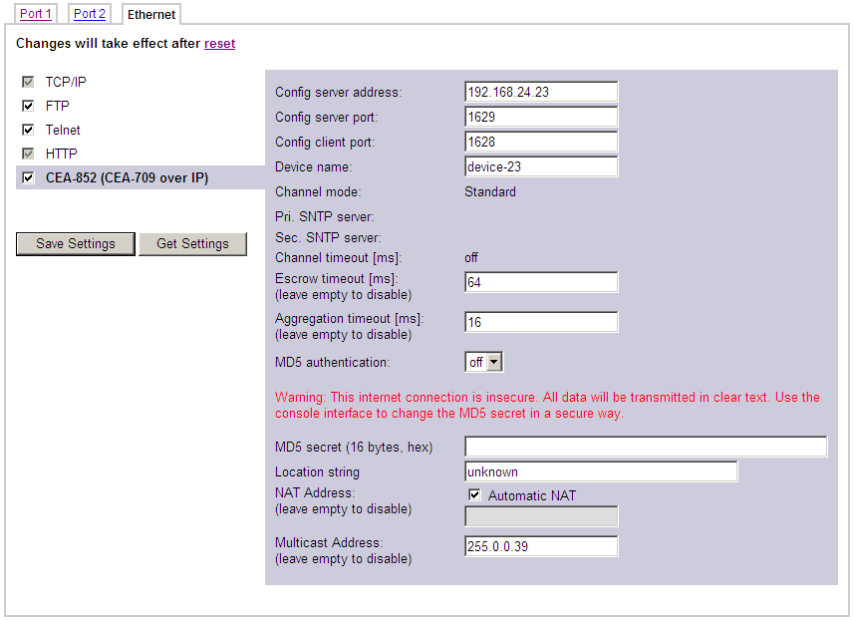


Abbildung 65: CEA-852-Geräte-Konfigurationsseite.

Die Felder **Config server address** und **Config server port** zeigen die IP-Adresse und den Port des Konfigurationsservers, welcher den L-IP und den IP-Kanal verwaltet. Das Feld **Config Client Port** repräsentiert den IP-Port der CEA-852-Einheit des Geräts. Diese Einstellung sollte auf dem Standardwert (1628) gelassen werden, außer es befinden sich mehr als ein CEA-852-Gerät hinter demselben NAT-Router. Lesen Sie bitte den Abschnitt 8.3, um mehr über die NAT-Konfiguration zu erfahren.

Um das Gerät zu identifizieren, kann der Benutzer im Feld **Device Name** einen Namen für den L-IP eingeben, der dann im IP-Kanal aufscheinen wird. Der Gerätename kann bis zu 15 Zeichen lang sein. Es wird empfohlen, für den ganzen IP-Kanal eineindeutige Namen zu verwenden.

Der aktuelle Kanalmodus der CEA-852-Einheit wird im Feld **Channel mode** angezeigt. Der Kanalmodus wird vom Konfigurationsserver eingestellt. Wenn sich im Kanal zwei Geräte mit derselben IP-Adresse, aber mit unterschiedlichen Portnummern befinden (z.B. mehrere CEA-852-Einheiten hinter demselben NAT-Router), wird der Kanalmodus auf **Extended NAT Mode** umgeschaltet. Lesen Sie bitte den Abschnitt 8.3, um mehr über den „Extended NAT Mode“ im Konfigurationsserver zu erfahren.

Die **SNTP-Server**-Adresse und das **Channel timeout** (Kanalzeitüberschreitung) werden vom Konfigurationsserver gesetzt.

Das Feld **Escrow timeout** legt fest, wie lange der L-INX auf „out-of-sequence“ CEA-852-Datenpakete wartet, bis diese verworfen werden. Geben Sie hier bitte die Zeit in ms ein, oder ‚0’ um die Escrow-Zeitüberschreitung zu deaktivieren. Die maximal einstellbare Zeit beträgt 255 ms.

Das Feld **Aggregation Timeout** definiert das Zeitintervall, in dem mehrere CEA-709-Pakete zu einem einzelnen CEA-852-Datenpaket zusammengefasst werden. Geben Sie bitte die Zeit in ms ein, oder eine ‚0’ um die diese Aggregation zu deaktivieren. Die maximale Zeit beträgt 255 ms. Beachten Sie, dass die Deaktivierung der Aggregation sich negativ auf die Performance der CEA-852-Einheit des L-IP auswirken kann.

Das Feld **MD5 Authentication** aktiviert oder deaktiviert die MD5-Authentifizierung. Im folgenden Feld **MD5 Secret** geben Sie den 16-Byte-langen MD5-Schlüssel ein. Beachten Sie, dass aus Sicherheitsgründen der aktive MD5-Schlüssel nicht angezeigt wird. Die 16 Bytes können als Zeichenkette, mit oder ohne Leerzeichen zwischen den einzelnen Bytes, eingegeben werden, z.B.: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Anmerkung: *Beachten Sie, dass die MD5-Authentifizierung nicht zusammen mit dem* i.*LON 1000 von Echelon verwendet werden kann. MD5 kann jedoch mit dem* i.*LON 600 verwendet werden.*

Beachten Sie außerdem, dass die Eingabe des MD5-Schlüssels über das Web-Interface ein potentielles Sicherheitsrisiko darstellen kann. Da die Informationen über das Netzwerk übertragen werden, können diese von anderen mitgelesen werden. Es wird empfohlen, entweder ein ausgekreuztes Ethernet-Kabel zu verwenden.

Im Feld **Location String** kann der Benutzer einen bezeichnenden Text eingeben, der den physikalischen Ort des Geräts beschreibt. Ein Location String kann eine maximale Länge von 255 Zeichen haben. Der Location String ist optional und dient zu Informationszwecken.

Wenn die CEA-852-Einheit des L-IP hinter einem NAT-Router verwendet wird, so muss die öffentliche IP-Adresse des NAT-Routers oder die der Firewall bekannt sein. Um die NAT-Adresse automatisch zu erkennen, lassen Sie das **Auto-NAT**-Häkchen eingeschaltet.

Das **Multicast Address**-Feld erlaubt dem Benutzer, die CEA-852-Einheit an eine Multicast-Gruppe für den CEA-852-IP-Kanal hinzuzufügen. Geben Sie hier die IP-Multicast-Adresse ein. Um zu erfahren, wie Sie eine gültige Multicast-Adresse erhalten, kontaktieren Sie bitte Ihren Systemadministrator. Lesen Sie bitte den Abschnitt 8.3, um mehr über den Gebrauch von Multicast-Adressen in Ihrem Kanal zu erfahren.

7.3.13 CEA-709 Router-Konfiguration

Die Konfigurationsseite des CEA-709-Routers dient zum Konfigurieren des eingebauten Router-Modus. Es sind zwei Modi, der **Configured Router** und der **Smart Switch** Modus verfügbar. Das Gerät muss neu gestartet werden, um Änderungen auf dieser Seite zu übernehmen.

Der Modus **Configured Router** ist voreingestellt. Wählen Sie diese Einstellung aus, wenn der L-IP als ein Standart-CEA-709-Router fungieren soll, der dann über eine Netzwerkmanagementsoftware, wie z.B. über den NL-200 oder LonMaker, konfiguriert werden kann.

Der „Smart Switch“-Modus lässt es dem Gerät über, ein selbstlernender Router ähnlich dem des L-Switches zu sein. In dieser Konfiguration braucht der eingebaute Router nicht über ein Netzwerkmanagementsystem konfiguriert werden, ist jedoch gänzlich im Netzwerk erkennbar. Innerhalb einer „Plug&Play“-Umgebung ist dieser Modus gut anzuwenden. Der „Smart Switch“-Modus sollte nur in LAN-Netzwerken verwendet werden. Wenn dieser Modus ausgewählt wurde, dann hat die Seite zwei weitere Felder zur Konfiguration: **Subnet/node learning** and **Group learning**.

In der Standardeinstellung wird der Router-Modus über die DIP-Schalter bestimmt. Siehe Abschnitt 8.1 für weiterführende Informationen über die unterschiedlichen Router-Modi.

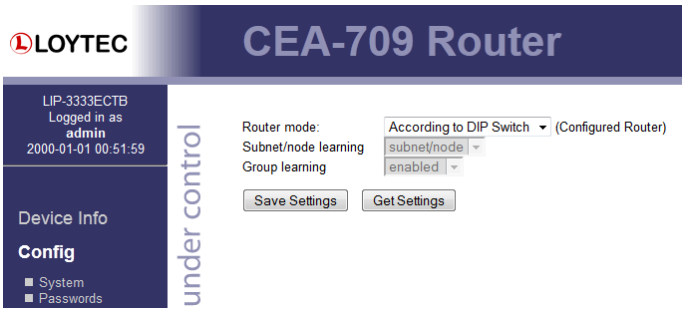


Abbildung 66: CEA-709 Router Konfiguratiosseite.

7.3.14 CEA-852 Server-Konfiguration

Auf dieser Seite kann der Konfigurationsserver des Geräts aktiviert oder deaktiviert werden. Im Drop-Down-Menü **Config server status** kann **enabled** ausgewählt und anschließend **Save Settings** gedrückt werden, um den Konfigurationsserver zu aktivieren. Danach erscheint die Konfigurationsseite des Konfigurationsservers wie in der Abbildung 67 zu sehen ist. Wenn der Konfigurationsserver aktiv ist, dann leuchtet die grüne Konfigurationsserver-LED, die mit **CS** am Gerät bezeichnet ist, anderenfalls bleibt die LED dunkel.

Der Port des Konfigurationsservers kann im Feld **Config server port** verändert werden. Es wird empfohlen, die Standardeinstellung auf 1629 zu belassen. Das Feld **Channel name** hat nur einen informellen Hintergrund und kann bis zu 15 Zeichen fassen.

Das **Channel members**-Feld zeigt die aktuelle Mitgliederanzahl am IP-852-Kanal an. Und das Feld **Channel mode** gibt den aktuellen Kanalmodus wieder. Der L-IP Konfigurationsserver bestimmt diesen Mode automatisch. Abhängig ist es davon, ob es zumindest zwei Geräte am Kanal, die die gleiche IP-Adresse, jedoch unterschiedliche Port-Adressen (z.B. mehrere L-IPs hinter einem NAT-Router) besitzen, gibt. Sollten alle IP-Adressen einmalig sein, dann ist der Modus auf **Standard**, wenn nicht, dann wird der Mode auf **Extended NAT mode** eingestellt. Sehen Sie im Abschnitt 8.3.2 nach, um mehr über die Auswirkungen dieses Modus zu erfahren.

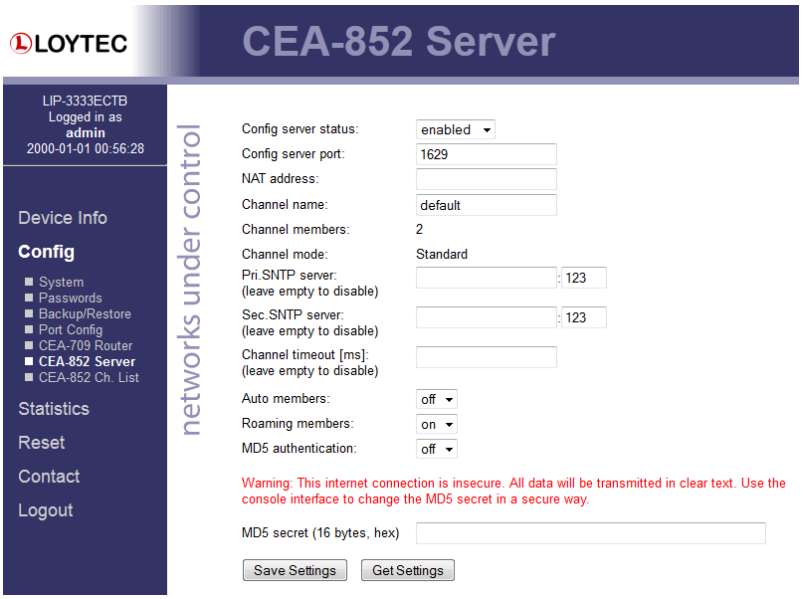


Abbildung 67: Konfigurationsserver-Einstellungen.

Geben Sie in den Feldern **Primary SNTP** und **Secondary SNTP** die Adressen von Zeitservern (NTP-Server) ein. Der L-IP wird sich dann über NTP mit dem spezifizierten, primären oder sekundären NTP-Server synchronisieren. Eine Liste verfügbarer Zeitserver in Ihrer Nähe finden Sie auf der Internetseite www.ntp.org.

Die Kanalzeitüberschreitung (**Channel timeout)** ist eine Eigenschaft des IP-852-Kanals und gibt an, wie alt ein Datenpaket sein muss, damit es verworfen werden kann. Die Kanalzeitüberschreitung ist in ms angegeben. Um diese Eigenschaft der Zeitüberschreitung abzustellen, braucht nur der Wert ‚0' eingegeben werden. Um einen angemessenen Wert einzugeben, sehen Sie im Abschnitt 8.5 nach. Einstellungen ungleich 0 benötigen einen gültigen SNTP-Servereintrag im Konfigurationsserver.

Mit der Option **Auto members** kann man Mitglieder automatisch zu einem Kanal anfügen. Wenn dies eingeschaltet wird, können CEA-852-Geräte auf einem IP-852-Kanal registriert werden, ohne dass diese Geräte explizit zum Konfigurationsserver eingetragen wurden. Diese besondere Eigenschaft ist in Kombination mit einem LPA-IP (LOYTEC Protokollanalysator) sehr wertvoll, da dieser sich selbst während einer Fehlersuche in den Konfigurationsserver einträgt. Auto-Mitglieder, die nicht mehr ansprechbar sind, werden automatisch von dem Kanal entfernt. Diese „Auto member support"-Eigenschaft entspricht nicht der Voreinstellung und muss bei Verwendung extra eingeschaltet werden. Verwenden Sie diese Eigenschaft mit großer Vorsicht, da neue CEA-852-Geräte sich selbst zu dem Kanal anhängen, ohne dass ein Systemintegrator oder Benutzer davon in Kenntnis gesetzt wird. Dieses Merkmal kann eine potentielle Sicherheitslücke darstellen.

Mit der Option **Roaming members** wird ein Verfolgen von CEA-852-Geräten erlaubt, wenn ihre IP-Adresse sich ändert. Diese Option muss eingeschaltet werden, wenn DHCP benutzt wird und der DHCP-Server verschiedene IP-Adressen auf ein und dasselbe Gerät (gleiche Neuron-ID) vergibt. In Verbindung mit Auto-NAT können L-IP-Geräte auch hinter NAT-Routern sitzen, die ihre IP-Adresse zwischen Verbindungsaufbauten ändern. Im Abschnitt 8.3.1 wird auf diese Eigenschaft näher eingegangen. Diese „roaming member feature"-Eigenschaft ist bereits voreingestellt. Wenn DHCP nicht verwendet wird oder wenn der DHCP-Server immer die gleiche IP-Adresse einer MAC-Adresse zuteilt, wird empfohlen diese Option auszuschalten.

Mit einem Drop-Down-Menü kann die **MD5 authentication** ein- oder ausgeschaltet werden. Sollte die MD5-Authentifizierung eingeschaltet sein, so müssen alle Geräte auf diesem IP-852-Kanal diese Eigenschaft der MD5-Authentifizierung aktiviert haben und den gleichen MD5-Schlüssel (MD5 secret) verwenden. Der MD5-Schlüssel kann über das Web-Interface

eingegeben werden. Die 16 Bytes können als Zeichenkette, mit oder ohne Leerzeichen zwischen den einzelnen Bytes, eingegeben werden: z.B.: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Anmerkung: *Wir weisen darauf hin, dass die MD5-Authentifizierung nicht zusammen mit einem* i.*LON 1000 verwendet werden kann. MD5 kann jedoch mit einem* i.*LON600 verwendet werden.*

Es wird empfohlen, dass der MD5-Schlüssel im lokalen Netz und nicht über eine Internet-Verbindung eingegeben wird. Am besten solle ein ausgekreuztes Ethernet-Kabel zum PC verwendet werden.

7.3.15 CEA-852 Channel List

Wenn der Konfigurationsserver auf dem Gerät aktiv ist, dann kann die CEA-852-Geräteliste im Menü CEA-852 Channel List aufgerufen werden. Ein Beispiel dazu sehen Sie in der Abbildung 68.

Die Schaltfläche **Add Device** wird benötigt, um ein weiteres CEA-852-Gerät auf den IP-852 einzubinden. Mit der Schaltfläche **Reload** wird die Seite neu geladen und aufgefrischt, mit **Recontact** werden alle Geräte verständigt und es werden ihre jeweiligen Status eingeholt. Die Schaltfläche **Execute** bewirkt, dass die Option, die im daneben liegenden Drop-Down-Menü ausgewählt wurde, für alle ausgewählten Zeilen ausgeführt wird. Jeder Teilnehmer kann für diesen Vorgang mittels eines individuellen Häkchens in der **Sel**-Spalte ausgewählt werden. Es stehen verschiedene Aktionen zur Auswahl: **disable**, **enable**, **delete**, **assign to NAT** und **remove from NAT**. Mehr über diese Aktionen erfahren Sie im Abschnitt 8.3.2.

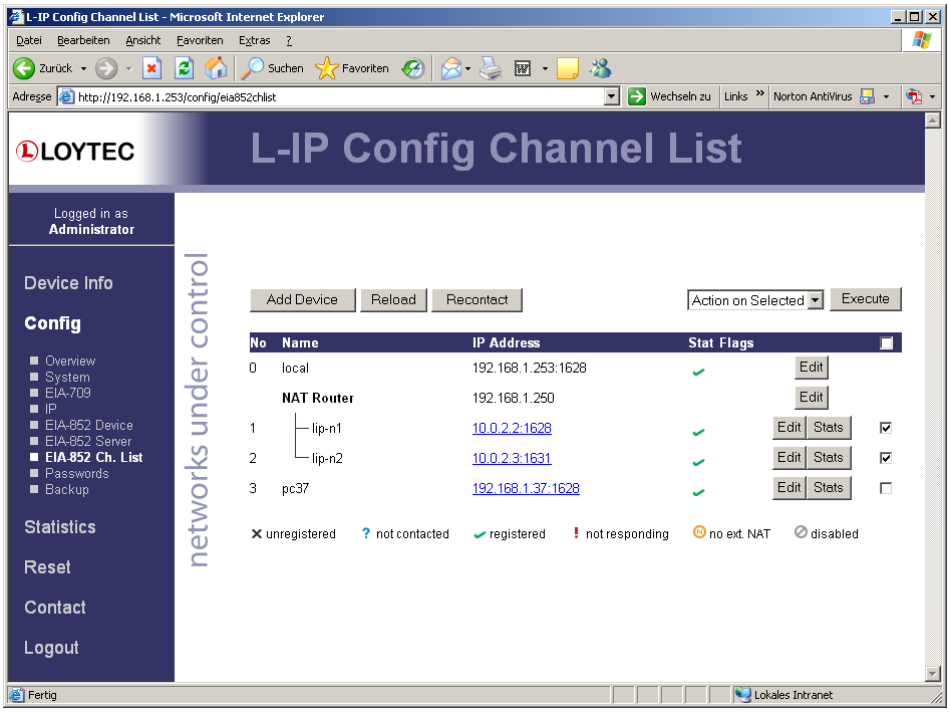


Abbildung 68: Mitgliederliste des CEA-852-Kanals.

Der Gerätestatus wird mittels anschaulichen Bildchen unterschiedlicher Farbe dargestellt. Eine Erklärung der unterschiedlichen Statusinformationen sehen Sie in Tabelle 5. In der Spalte **Flags** zeigt das Kennzeichen **A** an, dass das Gerät ein Automitglied ist.

Klicken Sie auf **Edit** um den Gerätenamen, die IP- und die Port-Adresse des Geräts zu ändern. Wenn Sie auf **Edit** bei einem NAT-Router klicken, dann können Sie dort die NAT-

Routeradresse verstellen. Die Schaltfläche **Stats** fragt die Statistik-Zusammenfassung eines Client-Geräts ab.

Icon	Status	Beschreibung
✔	registered	Das CEA-852-Gerät wurde erfolgreich auf dem IP-852-Kanal registriert und ist vollständig betriebsbereit.
✖	unregistered	Das CEA-852-Gerät wurde noch nie am IP-852-Kanal registriert.
?	not contacted	Das CEA-852-Gerät wurde seit dem Start des Konfigurationsservers noch nicht kontaktiert.
!	not responding	Das CEA-852-Gerät wurde registriert, kann jedoch derzeit nicht angesprochen werden.
⊘	disabled	Das CEA-852-Gerät wurde am Kanal deaktiviert (disabled oder rejected).
N	No extended NAT	Das CEA-852-Gerät unterstützt keinen „extended NAT“-Modus. Das Gerät ist deaktiviert.

Tabelle 5: Mögliche Kommunikationsprobleme bei einem Konfigurationsserver.

7.3.16 SSH-Server-Konfiguration

Auf Geräten, die einen SSH-Server enthalten, kann dessen Konfiguration auf der Ethernet-Seite verändert werden, wie in Abbildung 69 gezeigt.

Der SSH-Server kann aktiviert oder deaktiviert werden. Der TCP-Port des SSH-Servers kann ebenfalls verändert werden. Der Standard-SSH-Port ist 22. Diese Einstellungen werden erst nach einem Neustart gültig.

Die SSH-Server-Seite zeigt die aktuellen Fingerprints der RSA- und DSS-Host-Keys an. Jedes Gerät hat standardmäßig einen zufälligen DSS-Key (immer 1024 Bit) und einen zufälligen RSA-Key (1024 Bit). Dieser kann neu erzeugt werden, indem die gewünschte **RSA-Schlüssellänge** (1024 oder 2048 Bit) ausgewählt und die Schaltfläche **Erzeugen** gedrückt wird. Zusätzlich können auch EC-Keys erzeugt werden. Wählen Sie dazu die EC-Schlüssellänge in der Auswahlliste und drücken auf die Schaltfläche **Erzeugen**. Der SSH-Server lädt den neuen Host-Key beim nächsten Neustart.

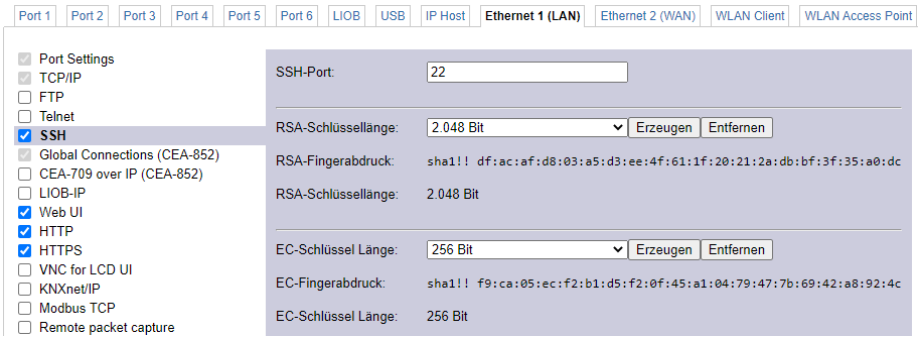


Abbildung 69: SSH Konfiguration.

Das Generieren der SSH-Keys kann bis zu einer Minute dauern. SSH-Clients, die den alten Host-Key bereits akzeptiert haben, verweigern die Verbindung mit dem Server, bis Sie die Änderung im Client bestätigen.

7.3.17 SNMP

Das Gerät verfügt über einen eingebauten SNMP Server. Alle System-Register und als OPC verfügbare Datenpunkte sind auch als Variablen in der SNMP Management Information Base (MIB) enthalten. Die MIB-Definition kann vom Web-Interface geladen werden, wie in

Abbildung 70 gezeigt wird. Man kann zwischen einem Text- und XML-Format wählen, jenachdem welches SNMP-Werkzeug verwendet wird. Für weiterführende Informationen zu SNMP auf dem Gerät lesen Sie bitten den Abschnitt 11.1.

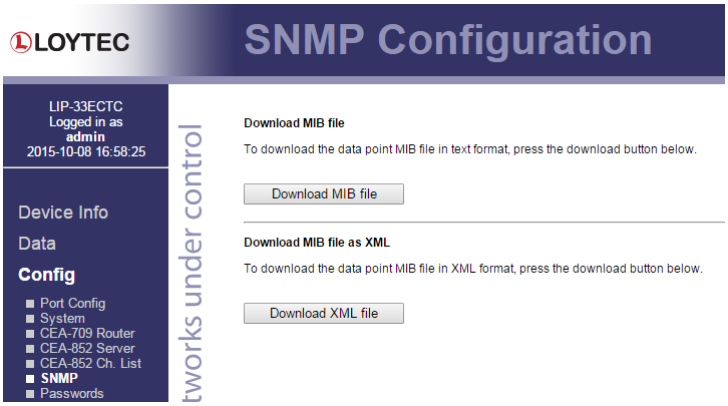


Abbildung 70: Laden der SNMP MIB vom Web-Interface

7.3.18 VPN-Konfiguration

Um das Interface für ein virtuelles, privates Netzwerk (VPN) auf dem LOYTEC-Gerät zu aktivieren, gehen Sie auf den Reiter **VPN** in der Portkonfiguration. Das VPN nutzt die OpenVPN-Technologie und kann in einem von zwei Modi konfiguriert werden: 1) Im VPN Client-Modus verbindet sich das Gerät zu einem VPN-Server und wählt sich in ein VPN ein. 2) Der VPN Simple Server-Modus aktiviert einen eigenen VPN-Server auf dem LOYTEC-Gerät und bietet eine OpenVPN-Konfiguration zum Download, die in anderen OpenVPN-Clients zur Verbindung auf das LOYTEC-Gerät verwendet wird. Diese Grundeinstellung wird über **OpenVPN Modus** gemacht, wie in Abbildung 71 gezeigt.

Wählen Sie **Client-Verbindung** aus und klicken Sie auf **Einstellungen speichern**, um den VPN-Client zu aktivieren. Optional setzen Sie den Haken bei **Lokales Subnetz routen**, damit das LOYTEC-Gerät den VPN-Verkehr auch zum und vom lokalen IP-Subnetz routet. Damit werden Geräte am lokalen IP-Netzwerk effektiv in VPN sichtbar, wenn der IP-Adressbereich vom Subnetz im gesamten VPN eindeutig ist (d.h. jede Liegenschaft ihr eigenes, eindeutiges IP-Subnetz hat, das geroutet werden kann).

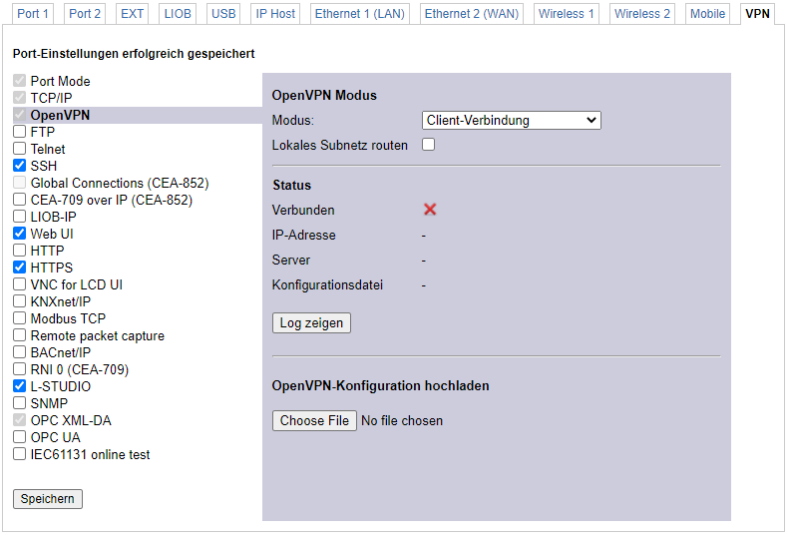


Abbildung 71: OpenVPN Client-Konfiguration.

Unter **OpenVPN-Konfiguration hochladen** klicken Sie auf den Knopf zum Auswählen einer Datei und wählen eine OpenVPN-Konfigurationsdatei (.ovpn) aus, die von einem OpenVPN-Server bereit gestellt wurde. Dann klicken Sie auf **Upload**, um die ovpn-Datei auf das LOYTEC-Gerät zu laden. Gebräuchliche OpenVPN-Server wie z.B. OpenVPN Access Server oder Synology OpenVPN werden unterstützt.

Anmerkung: *OpenVPN-Konfigurationsdateien müssen eingebettete Zertifikate haben und Auto-Login unterstützen, d.h. es darf keine Passworteingabe erzwungen werden, bevor eine Verbindung zu einem OpenVPN-Server aufgebaut wird.*

Während der Verbindung zum OpenVPN-Server wird die **Status**-Information aktualisiert. Letztendlich sollte der Status auf „verbunden“ stehen und die zugewiesene IP-Adresse im VPN angezeigt werden (siehe Abbildung 72). Um detailliertere Informationen über den Verbindungsaufbau oder zur Fehlersuche zu erhalten, klicken Sie auf den Knopf **Log zeigen**. Damit wird das Verbindungsprotokoll geladen.

Auf der Registerkarte VPN des Web-Interface für die Portkonfiguration können bestimmte Protokolle so konfiguriert werden, dass sie auf das VPN anstelle des lokalen Ethernet gebunden werden. Dies sichert ansonsten unsichere Protokolle wie CEA-852, BACnet/IP oder Modbus TCP. Aktivieren Sie dazu den VPN-Port im separaten Netzwerkmodus. Beachten Sie, dass für CEA-852 alle Clients und der Konfigurationsserver so konfiguriert sein müssen, dass sie auf die VPN-Schnittstelle gebunden sind. Wenn Sie BACnet/IP auf VPN binden, muss beachtet werden, dass auf dem OpenVPN-Server ein BBMD mit allen BACnet VPN-Clientadressen konfiguriert werden muss. Der LWEB-900 VPN-Server integriert einen automatisch konfigurierten BBMD und bietet somit eine Plug-and-Play-Lösung für BACnet/IP auf VPN.



Abbildung 72: VPN-Client Verbindungsstatus.

Wählen Sie **LWEB-900-Registrierung** aus, um sich bei einem LWEB-900-VPN zu registrieren, und klicken Sie auf **Einstellungen speichern**. Anstatt eine Konfigurationsdatei auf das Gerät zu laden, geben Sie den Projekt-PIN-Code für das LWEB-900 VPN ein und optional den Geräte-PIN-Code. Klicken Sie auf **Start**, um das LWEB-900-VPN zu suchen und das Gerät darin zu registrieren.

Wählen Sie den Modus **Simple Server**, um den OpenVPN-Server am LOYTEC-Gerät zu aktivieren. Geben Sie jene IP-Adresse/Hostnamen und Port ein, über die das LOYTEC-Gerät von extern erreichbar ist (siehe Abbildung 73). Der Port wird mit dem lokalen HTTPS-Port am Gerät geteilt. Bearbeiten Sie optional die **VPN-Adresse** des Servers. Dies ist hilfreich, wenn ein Client gleichzeitig eine Verbindung zu mehreren VPN-Servern herstellen möchte. Dann klicken Sie auf **Einstellungen speichern** und starten das Gerät neu, damit der VPN-Server aktiv wird. Beachten Sie bitte, dass die Einstellung einer Port-Weiterleitung für HTTPS auf dem NAT-Router erforderlich sein kann, damit das LOYTEC-Gerät von extern erreichbar ist.

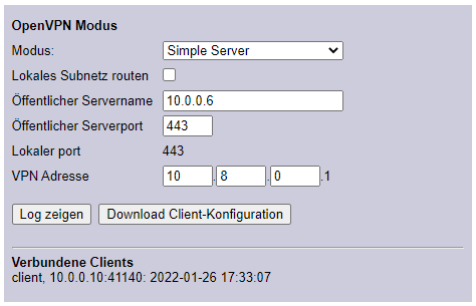


Abbildung 73: Konfiguration des OpenVPN Simple Server-Modus.

Nach dem Neustart ist der OpenVPN-Server am Gerät aktiv. Laden Sie die Client-Konfiguration durch einen Klick auf **Client-Konfiguration laden**. Importieren Sie diese Konfigurationsdatei in den OpenVPN-Client (z.B. die OpenVPN App auf einem Mobilgerät oder in die OpenVPN GUI am PC). Das Web-Interface im Simple Server-Modus zeigt Informationen über **Verbundene Clients** an. Derzeit kann nur ein Client gleichzeitig verbunden sein.

7.3.19 LTE-Konfiguration

LOYTEC-Geräte, die den LTE-800-Adapter unterstützen, können zum Anmelden bei einem mobilen LTE-Netzwerk verwendet werden. Um den LTE-800-Adapter auf dem LOYTEC-Gerät zu aktivieren, müssen Sie zunächst auf der Registerkarte **Mobile** der Portkonfiguration den Portmodus „Getrenntes Netzwerk“ auswählen (siehe Abbildung 74) und auf **Speichern** klicken.

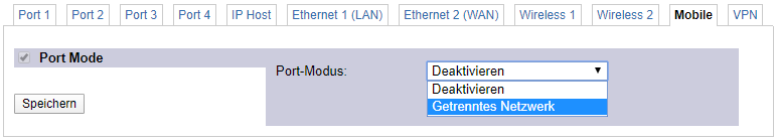


Abbildung 74: LTE über den Portmodus einschalten

Dadurch wird die LTE-Schnittstelle aktiviert und es wird zum Detail-Bereich für die Einstellungen für **Mobile Network** gesprungen (siehe Abbildung 75). Geben Sie abhängig von den von Ihrem Mobilfunkanbieter bereitgestellten Informationen die **APN** und zusätzlich **Benutzername** und **Passwort** ein, falls dies von Ihrem Mobilfunkanbieter verlangt wird. Geben Sie dann den **PIN Code** der SIM-Karte ein. Wenn die PIN-Funktion auf der SIM-Karte deaktiviert ist, lassen Sie dieses Feld leer. Aktivieren Sie **Roaming**, wenn Ihr Mobilfunkanbieter Roaming im Heimnetzwerk benötigt. Klicken Sie dann auf **Speichern**. Ob die SIM-Sperre erfolgreich entfernt wurde, wird im Statustext neben dem Feld PIN-Code angezeigt.

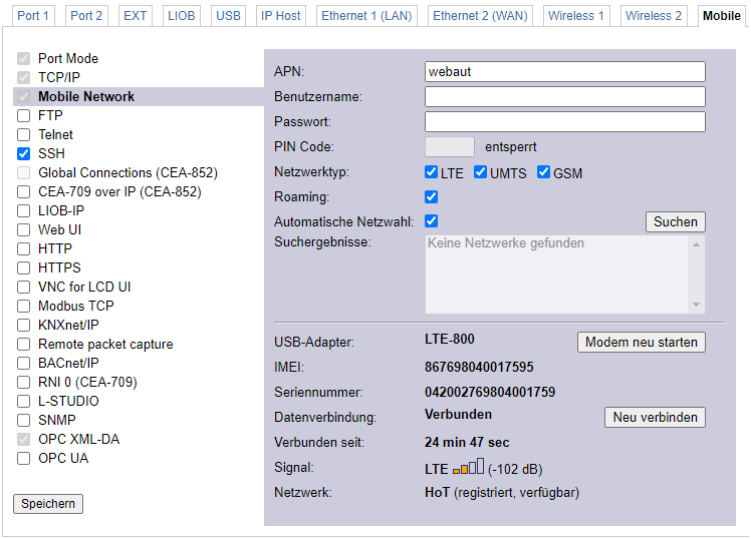


Abbildung 75: Einstellungen für das LTE-Mobilnetz.

Die LTE-Schnittstelle versucht nun, eine Datenverbindung zum Home-Netz herzustellen. Die Statusinformationen der LTE-Schnittstelle werden im unteren Teil des Detailbereichs **Mobile Network** angezeigt. Das Feld **Datenverbindung** zeigt schließlich „Verbunden“ an. Weitere Informationen zur **Signal**-Qualität und zum Mobilfunkbetreiber werden ebenfalls angezeigt. Informationen zum verbrauchten Datenvolumen finden Sie in der Mobilfunkstatistik (Abschnitt 7.2.6).

Zu Testzwecken ermöglicht die Schaltfläche **Neu verbinden** das Zurücksetzen und erneute Verbinden der LTE-Datenverbindung. Mit der Schaltfläche **Modem neu starten** können Sie das LTE-Modem komplett neu starten. Während des normalen Betriebs sind diese Aktionen nicht erforderlich.

Wenn ein anderer Netzbetreiber als das Heimnetzwerk verwendet werden soll, deaktivieren Sie das Kontrollkästchen **Automatische Netzwahl** und klicken Sie auf die Schaltfläche **Suchen**, um andere Mobilfunknetze zu finden. Die Liste der **Suchergebnisse** enthält die gefundenen Netzwerke (siehe Abbildung 76).

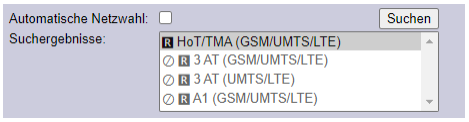


Abbildung 76: Suchergebnisse der Mobilnetze

Die Symbole in der Ergebnisliste haben folgende Bedeutung:

- ⌂ Heim-Netz
- ⃠ Nicht erlaubt (fremdes Netz)
- 🅁 Roaming: Um dieses Mobilnetz zu verwenden, aktivieren Sie auch das Kontrollkästchen **Roaming**.

Wählen Sie das gewünschte Netzwerk und speichern Sie die Einstellungen. Das Modem stellt über das neue Mobilfunknetz eine Verbindung her.

7.4 Sicherheit

7.4.1 Ändern der Passwörter

Die Passwörter für die Admin- und Operator-Konten wurden bereits beim ersten Kontakt zum Gerät gesetzt. Passwörter für lokal erstellte Benutzer wurden beim Erstellen des Benutzers festgelegt. Um das Passwort des aktuell angemeldeten Benutzers zu ändern, klicken Sie auf **Passwörter** unter dem Menüpunkt **Sicherheit**, was die Passwort-Konfigurationsseite öffnet, wie in Abbildung 77 gezeigt wird.



Abbildung 77: Passwort-Konfigurationsseite

Ist der Admin-Benutzer angemeldet, dann kann dieser auch das Operator- und Guest-Passwort ändern. Um das Admin-Passwort zu ändern, selektieren Sie das **admin**-Konto in der Auswahlbox und geben Sie das neue Passwort ein. Ein Indikator zeigt die Stärke des Passworts an, welche über die Sicherheit Auskunft gibt. Wenn das Passwort leer gelassen wird, ist der Passwortschutz deaktiviert und jeder kann auf das Gerät zugreifen, ohne ein Passwort eingeben zu müssen. Klicken Sie auf **Passwort ändern**, um die Änderung zu aktivieren.

Wenn der Admin-Benutzer angemeldet ist, klicken Sie auf **Alle Passwörter löschen**, um alle Passwörter auf dem Gerät zu löschen. Nach dem Löschen der Kennwörter müssen neue Administrator- und Operator-Passwörter festgelegt werden, bevor Sie mit dem Web-Interface weiterarbeiten können. Passwörter lokal angelegter Benutzer werden dadurch nicht gelöscht.

7.4.2 Zertifikate Verwalten

Einige L-IP Modelle unterstützen zusätzlich zu HTTP und OPC XML-DA die sicheren Protokolle HTTPS und OPC UA. Mit diesne kann verschlüsselt und authentifiziert kommuniziert werden.

Die HTTPS-Einstellungen können auf der Ethernet-Seite konfiguriert werden. Der HTTPS-Server kann aktiviert oder deaktiviert und sein TCP-Port verändert werden. Der Standard-HTTPS-Port ist 443. Diese Einstellungen werden erst nach einem Neustart gültig.

Wenn Sie sich mit einem Web-Browser per HTTPS mit dem Gerät verbinden, bekommen Sie eine Warnung, dass das Serverzertifikat ungültig oder selbstsigniert (self-signed) ist. Um die Verbindung aufzubauen, müssen Sie das Serverzertifikat akzeptieren oder bei einigen Browsern eine Ausnahme genehmigen.

Beachten Sie, dass in der Standardkonfiguration die Verbindung verschlüsselt, aber nicht sicher authentifiziert ist, da das Standardzertifikat der Firmware selbstsigniert und auf den Common Name „loytec.local“ ausgestellt ist. Falls Sie das Geräte in einer sicheren Umgebung betreiben und die Clients dies akzeptieren, sind keine weiteren Schritte notwendig.

Manche OPC UA Clients erlauben es beispielsweise aber nicht, das LOYTEC-Gerät über sein Standardzertifikat zu validieren. In diesem Fall muss der Common Name im selbstsignierten Zertifikat explizit die IP-Adresse oder den Host-Namen ausweisen, der für die Verbindung mit dem Client verwendet wird.

Zum Erstellen eines personalisierten, selbstsignierten Zertifikats für das LOYTEC-Gerät:

1. Gehen Sie zur Konfigurationsseite **Zertifikate** und wählen den Reiter **Zertifikat erstellen**. Der Radio-Knopf **Selbst-signiert** ist vorausgewählt sowie alle notwendigen Angaben wie in Abbildung 78 gezeigt. Beachten Sie, dass der **Common Name** jene IP-Adresse enthält, mit der das Gerät kontaktiert wurde. Haken Sie **EC-Schlüssel** an, wenn das Zertifikat EC anstelle von RSA verwenden soll.

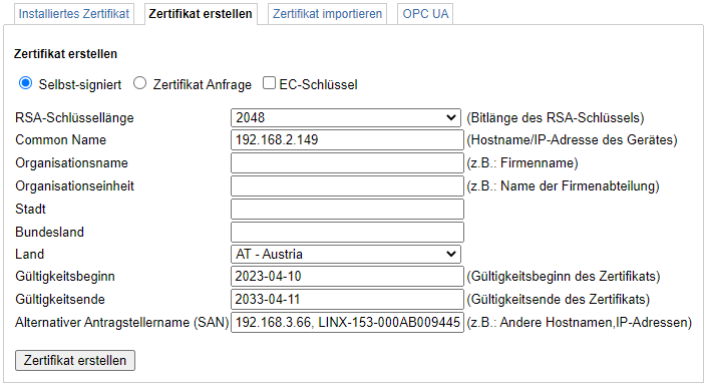


Abbildung 78: Erstellen eines personalisierten, selbstsignierten Zertifikats

2. Optional könne Sie die Felder nach Ihren Angaben modifizieren. Dann drücken Sie den Knopf **Zertifikat erstellen**. Die Erstellung kann bis zu einigen wenigen Minuten dauern. Nach Fertigstellung wird das selbstsignierte Zertifikat angezeigt (siehe Abbildung 79). Starten Sie das Gerät neu, um diese Änderung aktiv werden zu lassen.

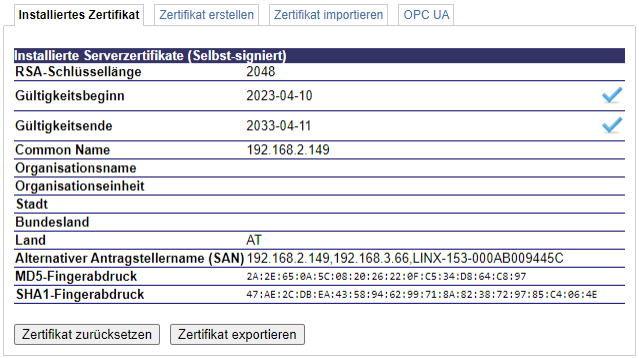


Abbildung 79: Neu erstelltes, selbstsigniertes Zertifikat

Um die Akzeptanz des LOYTEC-Servers in einer unsicheren Umgebung (wie etwa dem Internet) zu erhöhen, sollten Sie ein Zertifikat installieren, das von einer Certificate Authority signiert wurde, um Man-In-The-Middle-Angriffe zu vermeiden. HTTPS und OPC UA Server verwenden X.509-Zertifikate, um sich gegenüber ihren Clients zu authentifizieren. Um eine Verbindung aufzubauen, muss der Client das Server-Zertifikat akzeptieren. Hierzu gibt es zwei Möglichkeiten:

- Der Benutzer akzeptiert das Zertifikat manuell.
- Das Server-Zertifikat wurde von einer öffentlichen Certificate Authority (CA) erstellt.

LOYTEC-Geräte sind standardmäßig mit einem selbstsignierten Zertifikat ausgestattet, das aber durch ein eigenes Zertifikat ersetzt werden kann. Bitte beachten Sie folgende Schritte, um ein CA-signiertes Zertifikat zu installieren:

1. Gehen Sie auf die Konfigurationsseite **Zertifikate** und wählen den Reiter **Create Zertifikat erstellen**. Wählen Sie den Auswahlknopf **CA-Anfrage** wie in Abbildung 80 gezeigt. Im Feld **Common Name** geben Sie einen gültigen DNS Host-Namen (z.B. linx-g01.acme.com) oder die IP-Adresse für das Gerät ein. SSL-Zertifikate verwenden Host-Namen. Geben Sie weiters Organization Name, Organization Unit, City und State ein. Haken Sie **EC-Schlüssel** an, wenn das Zertifikat EC anstelle von RSA verwenden soll. Dann wählen Sie das Land und klicken auf den Knopf **Zertifikatsanfrage erstellen**.

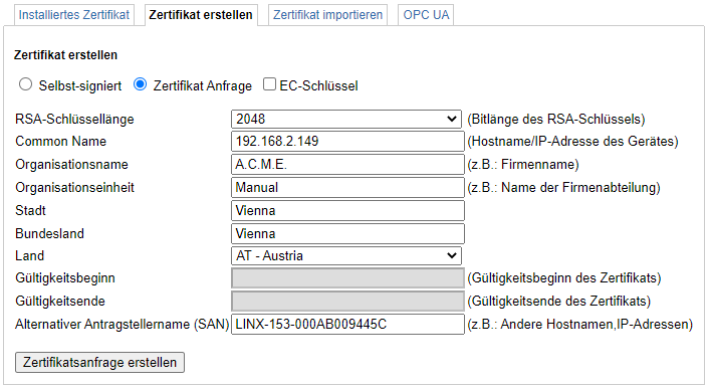


Abbildung 80: Erstellen einer Zertifikatanfrage an eine CA.

2. Kopieren Sie den X.509-Certificate-Request aus der Web-Seite wie in Abbildung 81 gezeigt und folgen Sie weiter der Anleitung, die Sie dazu von ihrer Certification Authority erhalten haben.

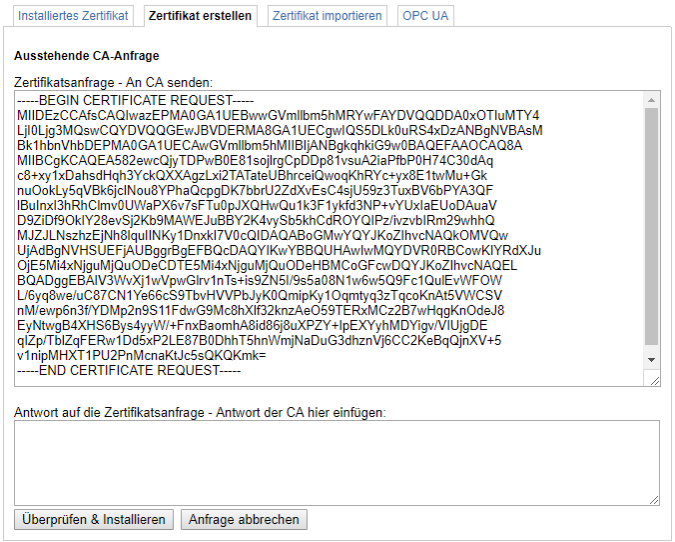


Abbildung 81: Kopieren der Anfrage für das X.509 Zertifikat.

3. Bestellen Sie das Zertifikat. Das Gerät benötigt das Zertifikat im PEM-Format, um es einfach einfügen zu können.

4. Nachdem Sie das Zertifikat erhalten haben, kopieren Sie es in die Zwischenablage. Dies sollte etwa so aussehen:

```
-----BEGIN CERTIFICATE-----
MIICyjCCAjOgAwIQEBBQUAMH4xCzAJBgNV…
```

```
… mehr Daten  …
-----END CERTIFICATE-----
```

5. Auf dem Reiter **Zertifikat erstellen** fügen Sie nun die kopierten Informationen in das Textfeld **Antwort auf die Zertifikatsanfrage** wie in Abbildung 81 gezeigt ein und klicken auf den Knopf **Überprüfen & Installieren**.

6. Nach einem Neustart lädt der HTTPS-Server das installierte Zertifikat, wodurch die Webseite des Geräts als vertrauenswürdig dargestellt wird.

7. Beachten Sie, dass Zertifikate eine beschränkte Gültigkeitsdauer von üblicherweise 1 oder 2 Jahren haben. Sie müssen diese Schritte wiederholen, bevor das Zertifikat ausläuft.

Alternativ können Sie ein Zertifikat auch aus einer Datei installieren. Dazu gehen Sie zum Reiter **Zertifikat importieren** wie in Abbildung 82 gezeigt. Wählen Sie die Datei mit dem Zertifikat im Feld **Server-Zertifikat** sowie die Datei mit dem privaten Schlüssel im Feld **Server privater Schlüssel** aus. Beide Dateien können im PEM- oder DER-Format vorliegen.

Wichtig!	***Sie können kein Server-Zertifikat ohne privaten Schlüssel installieren!***

Falls Ihre Zertifizierungsstelle ein Zwischenzertifikat verwendet importieren Sie dieses CA-Zertifikat im Feld **Zwischen-CA-Zertifikat** (selbes Format). Klicken Sie danach **Speichern**, um die Zertifikate zu importieren und zu speichern. Um ein installiertes Zertifikat wieder zu löschen, drücken Sie auf den Knopf **Zertifikat zurücksetzen** am Reiter **Installiertes Zertifikat**.

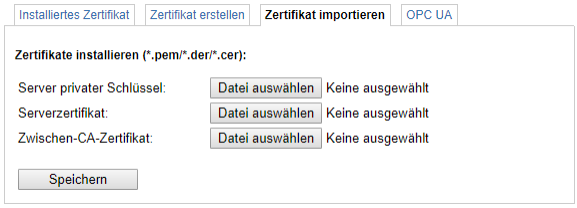


Abbildung 82: Installieren eines Zertifikats am Web-Interface.

7.4.3 Benutzerverwaltung

Das Gerät hat drei Benutzerkonten: (1) **guest** (Gast) erlaubt es dem Benutzer nur auf bestimmte Informationen, wie z.B. die Geräte-Informationsseite, zuzugreifen. Standardmäßig hat der Gastbenutzer kein Passwort gesetzt. Der (2) **operator** kann auf empfindlichere Daten wie die Kalenderdaten zugreifen und der (3) **admin** (Administrator) hat vollen Zugriff auf das Gerät und kann dessen Konfiguration verändern. Beachten Sie, dass diese Benutzerkonten ebenfalls verwendet werden, um sich in den SSH-, FTP- und Telnet-Server einzuloggen.

Es ist auch möglich, andere Benutzer lokal auf dem Gerät zu erstellen. Diese Benutzer können verschiedenen Rollen zugewiesen werden. Die Rollen ‚admin' und ‚operator' haben die gleichen administrativen Rechte wie ihre vordefinierten Gegenstücke, außer dass lokale Benutzer erstellt oder gelöscht werden dürfen. Es wird empfohlen, separate Benutzer mit der Rolle ‚admin' zu erstellen, um das Kennwort des Hauptadministrators geheim zu halten. Lokal erstellte Benutzer können jederzeit deaktiviert oder gelöscht werden, sodass bei Bedarf die Administratorrechte für einen von ihnen wieder entfernt werden können.

Die Rolle ‚lweb' kann Benutzern zugewiesen werden, die sich ausschließlich über die LWEB-802/803-Clients anmelden und im Rahmen des L-WEB-Visualisierungsprojekts arbeiten sollen. Diese Benutzer haben keine anderen administrativen Anforderungen an das Gerät.

Um lokale Benutzer zu verwalten, rufen Sie die Seite **Benutzerverwaltung** im Menü **Sicherheit** auf. Diese Seite zeigt die Liste der lokalen Benutzer an (siehe Abbildung 83). Das Verwalten lokaler Benutzer ist nur zulässig, wenn Sie mit dem Benutzerkonto ‚admin' angemeldet sind.

Klicken Sie auf **Benutzer hinzufügen**, um einen neuen Benutzer anzulegen und geben Sie **Benutzername**, **Passwort** und die **Rolle** in der Dropdown-Liste ein. Klicken Sie dann auf das Speichersymbol. Um das Passwort oder die Rolle eines lokalen Benutzers zu bearbeiten, klicken Sie auf das entsprechende Bearbeitungssymbol, aktualisieren Sie den Inhalt und klicken Sie auf das Speichersymbol.



Abbildung 83: Seite für die Benutzerverwaltung.

Andere Aktionen für lokale Benutzer umfassen Aktivieren, Deaktivieren und Löschen. Aktivieren Sie das Kontrollkästchen auf der rechten Seite für einen oder mehrere Benutzer und wählen Sie eine Aktion aus der Dropdown-Liste **Aktion ausführen** aus. Klicken Sie dann auf **Ausführen**. Deaktivierte Benutzer können sich nicht mehr anmelden, ihre Anmeldeinformationen verbleiben jedoch auf dem Gerät und können erneut aktiviert werden.

7.5 Dokumentation

Die **Documentation** Seite am Web-Interface erlaubt den Zugriff auf die das Gerät betreffende Dokumentation. Die auf dieser Seite angezeigten Dateien und Links können wie in Abschnitt 7.6.3 beschrieben konfiguriert werden.

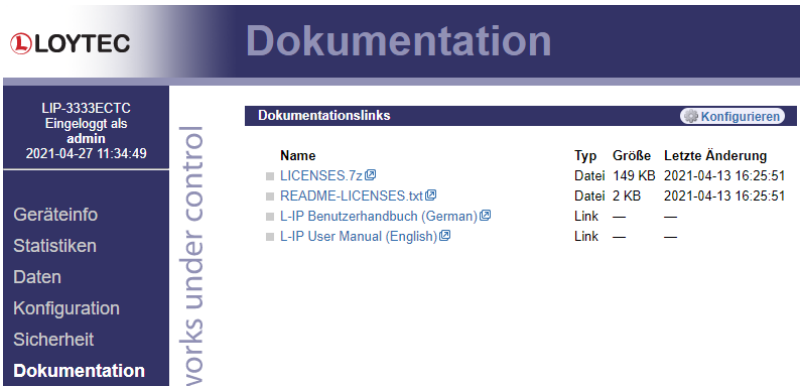


Abbildung 84: Web-Interface für den Zugriff auf die Gerätedokumentation.

Anmerkung: *Die auf über die **Documentation** Seite verfügbare Dokumentation ist für alle Nutzerkonten (inkl. Guest) erreichbar.*

7.6 Wartung

7.6.1 Konfigurationssicherung und Wiederherstellung

Eine Sicherung der Konfiguration des Geräts kann über das Web-Interface heruntergeladen werden. Drücken Sie auf den Backup/Restore-Link, wie in Abbildung 85 zu sehen ist und starten Sie den Ladevorgang. Das Gerät stellt eine Datei zusammen, die alle benötigten Teile enthält. Ein Datei-Dialog erscheint um den Speicherort der Sicherungsdatei einzugeben.

Bestimmte Inhalte eines Sicherungsarchivs können über Check Boxen kontrolliert werden. Standardmässig werden Passworte und IP-Einstellungen inkludiert. Wird der Haken von **Passwords** oder **IP settings** weggenommen, werden diese Inhalte vom Archiv exkludiert.

Um Geräteeinstellungen wiederherzustellen, braucht man nur die im Vorfeld abgespeicherte Sicherungsdatei im Bereich **Restore Configuration** mit Hilfe der Schaltfläche, die sich neben dem Feld **Filename** befindet, auswählen. Anschließend drücken Sie die Schaltfläche **Restore**. Wenn die Haken in den Restore-Optionen weggelassen werden, so werden die entsprechenden Inhalte nicht aus dem Archiv wiederhergestellt.

Die gesicherten Daten bestehen aus folgenden Teilen:

- IP-Einstellungen, wenn die Option angehakt ist,
- Benutzer und Passworte, wenn die Option angehakt ist,
- Geräteeinstellungen (Zeitzone, usw.),
- CEA-709 Kommissionierungsdaten,
- CEA-852 Geräte- und Configuration Server-Information (wenn eingeschaltet),
- L-IP Redundant Konfigurationsdaten (Knotenliste, Parameter, usw.),
- am Gerät abgelegte Dokumentationsdateien und –verknüpfungen.



Abbildung 85: Konfigurationssicherung und Wiederherstellung ─ Backup/Restore.

Anmerkung: *Sicherungen, die mit einer Firmware-Version vor Version 6.0 erstellt wurden, können auf Geräten mit Version 6.0 oder höher nicht wiederhergestellt werden! Bitte stellen Sie sicher, dass Sie die Sicherung erneut erstellen, nachdem Sie die Firmware aktualisiert haben!*

7.6.2 Firmware

Auf der Firmware-Seite können Sie die Firmware Ihres Geräts über das Web-Interface mit originalen LOYTEC Firmware-Images aktualisieren. Die Integrität des Images wird durch eine Firmware-Signatur sichergestellt. Die Weboberfläche bietet zwei Optionen:

- **Web Update**: Mit dem Web Update sucht das Gerät nach der neuesten verfügbaren Firmware auf dem LOYTEC Server. Klicken Sie auf das Aktualisierungs-Symbol, falls keine letzte Version angezeigt wird. Beachten Sie dabei bitte, dass am Gerät ein DNS-Server konfiguriert sein muss, um den LOYTEC Server zu finden. Drücken Sie auf den Knopf **Install** um die Aktualisierung durchzuführen.

- **Local file**: Aktualisieren Sie das Gerät mit einer lokalen Datei. Um das zu erreichen, wählen Sie eine .dl Datei auf der Festplatte aus und drücken auf den Knopf **Start Update**.



Abbildung 86: Firmware-Aktualisierung über das Web-Interface.

In beiden Fällen wird eine Gerätesicherung erstellt und in den lokalen Download-Ordner des Web-Browsers gespeichert, bevor die Aktualisierung startet. Soll keine Sicherung erfolgen, deselektieren Sie den Haken **Vor dem Firmware Update ein Backup herunterladen**.

7.6.3 Dokumentation

Auf der **Documentation** Seite im Menü **Wartung** können Dokumentationsdateien (z.B. Pläne) auf das Gerät geladen werden und Verknüpfungen (Links) zu externer Dokumentation angelegt werden. Die auf dieser Seite konfigurierte Dokumentationsinformation ist über den Menüpunkt **Documentation** im Hauptmenü verfügbar (siehe Abschnitt 7.5).

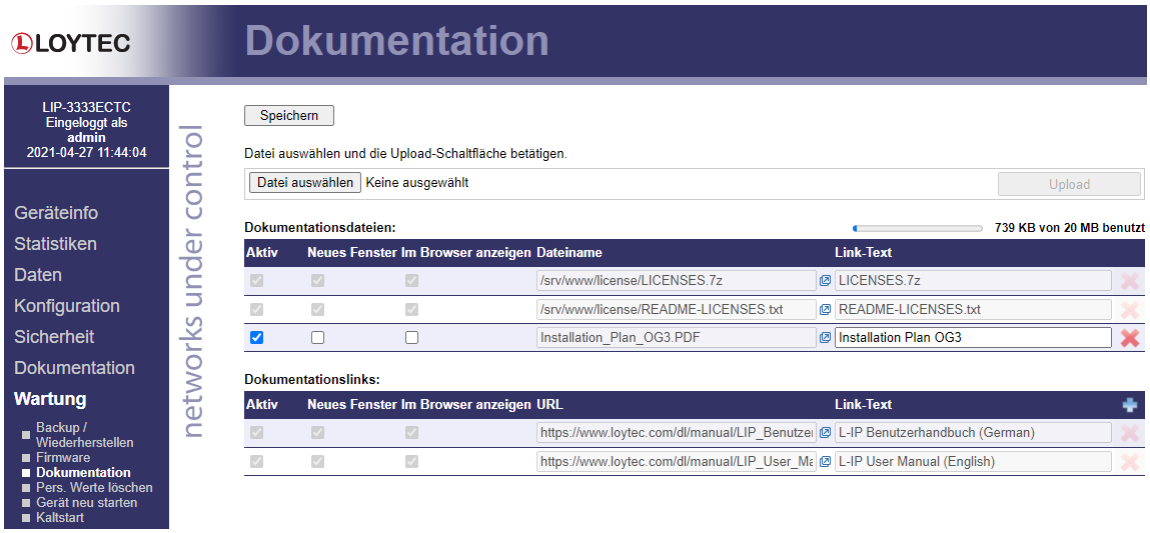


Abbildung 87: Ablage von Projekt-Dokumentation am Gerät.

Um Dokumentationsdateien auf dem Gerät abzulegen klicken Sie auf die Schaltfläche **Choose File**. Es öffnet sich ein Dateiauswahldialog. Wählen Sie die zu abzulegende Datei aus und klicken Sie auf **Upload** um den Transfer zu starten. Sobald die Übertragung erfolgreich abgeschlossen wurde erscheint die Datei im Bereich **Documentation files**. Ergänzen Sie den Eintrag mit einem Link-Text für die Anzeige der Datei auf der **Documentation** Seite.

Um einen Verweis auf eine externe Dokumentationsquelle hinzuzufügen klicken Sie auf das Symbol in der Kopfzeile des Bereichs **Documentation links**. Für jeden Eintrag in der Liste muss eine URL und ein Text für die Anzeige auf der **Documentation** Seite eingeben werden.

Links und Dateien können auf der Seite **Documentation** durch an- bzw. abhaken der Check-Box **Enabled** aktiv und inaktiv gesetzt werden. Inaktive Einträge, bei denen die Check-Box nicht gesetzt ist werden auf der Seite **Documentation** nicht angezeigt. Die Check-Box **New window** bestimmt ob der Link oder die Datei in einem neuen Browser-Tab geöffnet wird. Wenn **Show in browser** angehakt ist, so wird der Browser angewiesen die Datei wenn möglich selbst anzuzeigen. Andernfalls wird die Datei heruntergeladen. Um einen Link oder eine Datei zu entfernen klicken Sie auf das Symbol auf der rechten Seite der Liste. Um die Änderungen zu Speichern klicken Sie auf die Schaltfläche **Save**.

7.6.4 Neustart und Löschen von Daten

Der Menüpunkt **Wartung** ermöglicht die folgenden wichtigen Aktionen, um das Gerät neu zu starten oder Daten zu löschen:

- Neustart des Geräts per Fernzugriff. Verwenden Sie **Kaltstart**, um das Gerät wie nach einem Stromausfall neu zu starten, während das reguläre **Gerät neu starten** schneller ist und nur die Anwendung neu startet.

7.6.5 Sicherer Neustart

Immer wenn eine Einstellung geändert wird, die die Kommunikationsverbindung mit dem Web-Interface des Geräts beeinflussen kann (z.B. die IP-Adresse), wird er nächste Neustart als sicherer Neustart ausgeführt. Darauf wird wie in Abbildung 88 hingewiesen.



Abbildung 88: Hinweis auf einen sicheren Neustart.

Wenn das Gerät im sicheren Neustart-Modus gestartet wird, muss sich der Benutzer innerhalb von 5 Minuten in das Web-Interface einloggen. Eine Liste von möglichen, neuen IP-Adressen wird vorgeschlagen, um die Navigation auf die neue URL zu erleichtern. Wird innerhalb dieser Zeit kein Login erkannt (z.B., weil die neuen IP-Einstellungen die Verbindung unterbrochen haben), so wird das Gerät auf die zuvor funktionierenden Einstellungen zurückgesetzt.

7.7 Kontakt und Logout

Das Element **Kontakt** stellt unsere Kontaktinformationen vor und bietet einen Link auf das aktuellste Benutzerhandbuch, sowie der neuesten Firmware-Version. Der Menüpunkt **Logout** beendet die aktuelle Sitzung.

8 Betriebsarten des L-IP

Der L-IP routet CEA-709-Pakete über IP Netzwerke (Internet/Intranet). Abhängig vom Anwendungsfall des L-IP werden unterschiedliche Betriebsarten unterstützt, wie Pakete zwischen der CEA-709-Seite und der IP-Seite des L-IP geroutet werden. IP-seitig kann der L-IP als Client-Gerät, als Konfigurationsserver für den IP Kanal als auch als Client-Gerät und Konfigurationsserver zur gleichen Zeit eingesetzt werden.

8.1 CEA-709 Router - Operating Modes

Abhängig von den Einstellungen der DIP-Schalter 1 und 2 unterstützt der L-IP bis zu 4 unterschiedliche Arten, um Pakete zwischen dem CEA-709 und dem IP-Kanal zu routen. Die 4 Betriebsarten sind hier kurz angeführt und in den nachfolgenden Abschnitten genauer erläutert:

- OFF-OFF: Der L-IP verhält sich wie ein normaler konfigurierter CEA-709 Router (i.LON 1000/600-äquivalent)
- ON-ON: Der L-IP verhält sich wie ein selbstlernender Plug&Play-Router („Smart Switch Modus“)
- ON-OFF: Der L-IP verhält sich wie ein Store-und-Forward Repeater
- OFF-ON: Der L-IP lernt die Netzwerktopologie leitet aber keine Subnet-Broadcast adressierte Nachrichten weiter.

Wichtig: ***Der L-IP Redundant unterstützt nur den Configured Router Modus!***

8.1.1 Configured Router Modus

In dieser Betriebsart verhält sich der L-IP wie ein herkömmlicher, konfigurierter Router, der mit Standardnetzwerkmanagementwerkzeugen wie z.B. LonMaker oder NL-220 konfiguriert wird. Diese Betriebsart ist äquivalent zu dem *i*.LON 1000 Internet Server und dem *i*.LON 600 LONWORKS/IP Server.

Abbildung 89 zeigt die DIP-Schaltereinstellungen für den konfigurierten Router-Modus, unter der Annahme, dass alle anderen Schalter in der Werkseinstellung belassen wurden. Diese Einstellung ist die Werkseinstellung des L-IP bei Auslieferung des Gerätes. Die Modelle der L-IP C-Serie besitzen keine DIP-Schalter.

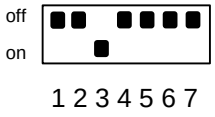


Abbildung 89: OFF-OFF: DIP-Schaltereinstellungen im konfigurierten Router-Modus (Werkseinstellung).

Diese Betriebsart verwendet die “Channel Routing” Routing-Strategie am IP Kanal. In dieser Betriebsart ist der L-IP vollkommen kompatibel mit dem *i*.LON 1000. Diese Betriebsart sollte in Netzwerken mit mehr als 10 L-IP Geräten am CN/IP Kanal und hohem Datenverkehrsaufkommen am CN/IP Kanal (mehr als 500 Pakete/s) verwendet werden, da „Channel Routing“ das IP-Paket nur an die L-IP-Geräte schickt, an denen die CEA-709 Knoten angeschlossen sind, die in diesem IP-Paket adressiert sind, und nicht zu allen L-IP-Geräten am CN/IP-Kanal. Dies ist die Standardbetriebsart des L-IP.

8.1.2 Smart Switch Mode

Der L-IP kann als selbstlernender Switch für CEA-709-Netzwerke konfiguriert werden. In dieser Betriebsart entscheidet der L-IP, basierend auf der Zieladresse im Datenpaket, ob das Datenpaket auf die andere Seite weitergeleitet werden soll oder nicht. Der L-IP isoliert somit den lokalen Netzwerkverkehr vom Netzwerkverkehr am Backbone. Diese Betriebsart wird „Smart Switch Modus“ genannt und ist besonders in Netzwerken mit hohen Paketraten von großer Bedeutung.

Abbildung 90 zeigt die DIP-Schaltereinstellungen, um den L-IP in den Smart Switch Modus zu setzen. Die Modelle der L-IP C-Serie besitzen keine DIP-Schalter.

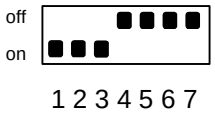


Abbildung 90: : ON-ON: DIP-Schaltereinstellungen für den Smart Switch Modus.

Achtung:	***Diese Betriebsart unterstützt keine Netzwerkschleifen!***

Achtung:	***Wird das Netzwerk umkonfiguriert, so ist es empfehlenswert, die Forwarding-Tabellen im L-IP durch Drücken des Statustasters für zumindest 20 s zu löschen (siehe Abschnitt 6.5.1).***

Der L-IP kann bis zu 4 Domains lernen.

Hinweis:	*Alle Pakete, die auf einer nicht gelernten Domain empfangen werden, werden an alle Ports weitergeleitet!*

Der Lernalgorithmus für Subnet/Node-Adressen sorgt für die Aufteilung des Netzwerkverkehrs basierend auf der Subnet/Node-Zieladresse einer Nachricht. Anders als bei herkömmlichen CEA-709-Routern muss der Anwender daher beim L-IP NICHT darauf achten, dass sich ein CEA-709-Subnet nicht über mehrere physikalische Netzwerksegmente erstrecken darf. Der L-IP erkennt auch, wenn ein Knoten von einem Segment in ein anderes versetzt wird und verändert die Netzwerktabellen entsprechend.

Hinweis:	*Alle Nachrichten mit einer noch nicht gelernten Subnet/Node-Zieladresse werden an alle Ports weitergeleitet!*

Der L-IP unterstützt das Lernen von Gruppenadressen. Gruppen dürfen sich über mehrere L-IP-Ports hinweg erstrecken.

Hinweis:	*Um Gruppenadressen lernen zu können, müssen gruppenadressierte Nachrichten entweder im bestätigten (acknowledged) oder im request/response Dienst gesendet werden.*

Hinweis:	*Alle Nachrichten mit einer noch nicht gelernten Gruppenzieladresse werden an alle Ports weitergeleitet!*

Der L-IP verfügt über keinen Lernalgorithmus für Broadcast-Adressen. Daher werden subnet- und domain-weite Broadcasts an alle Ports weitergeleitet.

Wenn subnetzweite Broadcasts nicht weitergeleitet werden sollen, verwenden Sie bitte den Smart Switch Modus ohne Weiterleiten von subnetzweiten Broadcasts (siehe Abschnitt 8.1.4).

Der L-IP verfügt über keinen Lernalgorithmus für Unique-Node-ID-Adressen („Neuron-ID“). Daher werden alle Nachrichten mit Unique-Node-ID-Adressen weitergeleitet.

Diese Betriebsart verwendet die “Channel Routing” Routing-Strategie am IP-Kanal. Es wird ein sogenanntes Flooding am IP Kanal verwendet, wobei alle Pakete am IP-Kanal an alle IP-Geräte (L-IP) auf diesem IP Kanal gesendet werden. Der Vorteil dieser Betriebsart ist, dass sie vollkommen Plug&Play ist und kein Netzwerkmanagement-Tool benötigt wird, um den L-IP zu konfigurieren. Der Nachteil dieser Betriebsart ist, dass sie für große Netzwerke nicht gut skaliert. Wir empfehlen diese Betriebsart für Netzwerke mit bis zu 10 L-IPs und einem Datenaufkommen von weniger als 500 Paketen/s. Bitte verwenden Sie den konfigurierten Router Modus aus Abschnitt 8.1.1 für große Netzwerke.

Es wird empfohlen, Multicast für L-IPs im Smart Switch Mode zu konfigurieren, um den Datenverkehr am Netz und in den Geräten zu senken und die Skalierbarkeit zu verbessern. Abschnitt 8.4 beschreibt die Konfiguration von Multicast am L-IP.

8.1.3 Store-and-Forward Repeater Mode

Der L-IP kann als Repeater konfiguriert werden. In dieser Betriebsart werden sämtliche Datenpakete unabhängig vom Adressformat weitergeleitet. Um den L-IP in den Repeater Modus zu versetzen, müssen folgende Schritte gemacht werden:

- DIP-Schalter 1 muss auf ON sein, siehe Installationsblatt des Produkts.
- DIP-Schalter 2 muss auf OFF sein, siehe Installationsblatt des Produkts.
- Die Forwarding-Tabellen müssen durch Drücken des Statustasters für zumindest 20 s gelöscht werden.

Abbildung 91 zeigt die DIP-Schaltereinstellungen für den Repeater-Modus, unter der Annahme, dass alle anderen DIP-Schalter in der Werkseinstellung belassen wurden. Die Modelle der L-IP C-Serie besitzen keine DIP-Schalter.

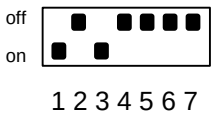


Abbildung 91: ON-OFF: DIP-Schaltereinstellungen für den Repeater-Modus.

Diese Betriebsart verwendet die “Channel Routing” Routing-Strategie am IP-Kanal. Es wird ein sogenanntes Flooding am IP-Kanal verwendet, wobei alle Pakete am IP-Kanal an alle IP-Geräte (L-IP) auf diesem IP Kanal gesendet werden. Der Vorteil dieser Betriebsart ist, dass sie vollkommen Plug&Play ist und kein Netzwerkmanagement-Tool benötigt wird, um den L-IP zu konfigurieren. Der Nachteil dieser Betriebsart ist, dass sie für große Netzwerke nicht gut skaliert. Wir empfehlen diese Betriebsart für Netzwerke mit bis zu 10 L-IPs und einem Datenaufkommen von weniger als 500 Paketen/s.

Es wird empfohlen, Multicast für L-IPs im Repeater Mode zu konfigurieren um den Datenverkehr am Netz und in den Geräten zu senken und die Skalierbarkeit zu verbessern. Abschnitt 8.4 beschreibt die Konfiguration von Multicast am L-IP.

8.1.4 Smart Switch Mode ohne Subnet-Broadcast Weiterleitung

Diese Betriebsart ist ähnlich dem Smart Switch Modus aus Abschnitt 8.1.2 mit dem Unterschied, dass subnetzweite Broadcasts nicht weitergeleitet werden. Diese Betriebsart kann in großen Netzwerken verwendet werden, wo ein Netzwerkmanagement-Tool Group-Overloading verwendet, um Gruppenadressen mit subnetzweiten Broadcasts zu ersetzen. In dieser Betriebsart muss der Systemintegrator sicherstellen, dass sich eine Subnetzadresse nur hinter einem einzigen Netzwerkanschluss verbirgt. Diese Bedingung ist erfüllt, wenn ein Netzwerk mit einem LNS-basierenden Netzwerkmanagement-Tool installiert wird, und die Knoten auf unterschiedlichen Kanälen (Channels) angeordnet werden, die mit einem Router Shape oder einem L-IP LonMaker Shape verbunden werden. Die LonMaker Shapes für den L-IP können von unserer Website www.loytec.com geladen werden.

Abbildung 92 zeigt die DIP-Schalter Einstellungen für den Smart Switch Modus ohne subnetzweite Broadcast-Weiterleitung. Alle anderen DIP-Schalter sind in der Werkseinstellung belassen. Die Modelle der L-IP C-Serie besitzen keine DIP-Schalter.

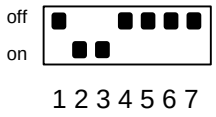


Abbildung 92: OFF-ON: DIP-Schaltereinstellungen für den Smart Switch Modus ohne subnetzweite Broadcast-Weiterleitung.

Diese Betriebsart verwendet die “Channel Routing” Routing-Strategie am IP-Kanal. Es wird ein sogenanntes Flooding am IP-Kanal verwendet, wobei alle Pakete am IP-Kanal an alle IP-Geräte (L-IP) auf diesem IP Kanal gesendet werden. Der Vorteil dieser Betriebsart ist, dass sie vollkommen Plug&Play ist und kein Netzwerkmanagement-Tool benötigt wird, um den L-IP zu konfigurieren. Der Nachteil dieser Betriebsart ist, dass sie für große Netzwerke nicht gut skaliert. Wir empfehlen diese Betriebsart für Netzwerke mit bis zu 10 L-IPs und einem Datenaufkommen von weniger als 500 Paketen/s.

Es wird empfohlen, Multicast für L-IPs im Smart Switch Mode zu konfigurieren um den Datenverkehr am Netz und in den Geräten zu senken und die Skalierbarkeit zu verbessern. Abschnitt 8.4 beschreibt die Konfiguration von Multicast am L-IP.

8.2 CEA-852 Betriebsarten

Jeder logische IP-Kanal benötigt einen Konfigurationsserver, der alle Geräte am CN/IP-Kanal (L-IP, LOYTEC NIC852, *i*.LON 1000, *i*.LON 600, LonMaker, etc.) verwaltet. Traditionellerweise wird dazu ein Windows PC verwendet, der als Konfigurationsserver dient. Der L-IP kann nun diesen PC ersetzen und parallel zu seiner normalen Funktionalität als Konfigurationsserver dienen. Das einfache Netzwerk in Abbildung 93 verwendet 2 L-IPs, um 2 CEA-709 Kanäle miteinander zu verbinden. Ein L-IP agiert als Router und als Konfigurationsserver für diesen Kanal. Der zweite L-IP agiert als normaler CEA-709 nach IP Router.

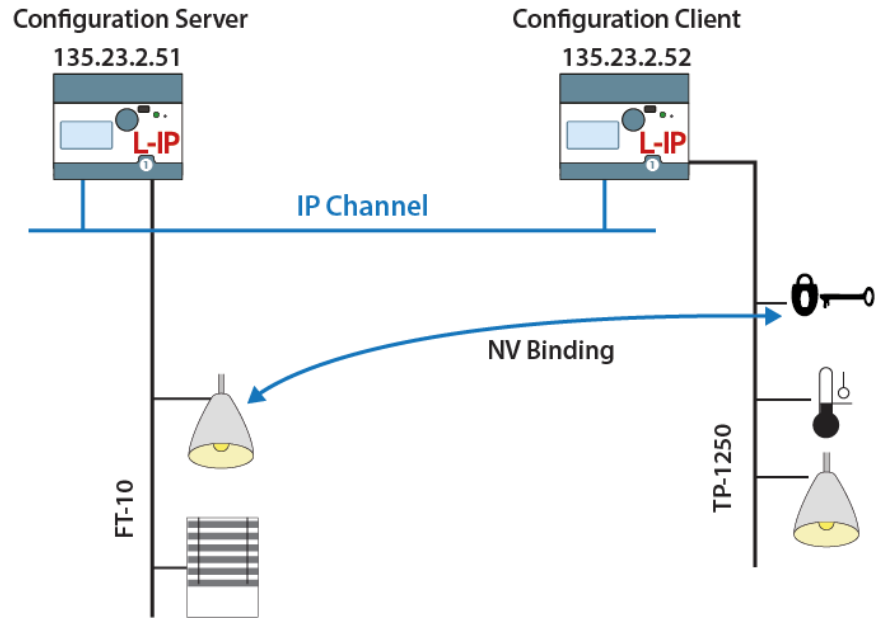


Abbildung 93: Der IP-Kanal besteht aus 2 IP-Geräten. Der linke L-IP mit IP-Adresse 135.23.2.51 agiert als Router und als Konfigurationsserver für den CN/IP-Kanal. Er verwaltet beide IP-Geräte 135.23.2.51 und 135.23.2.52.

8.2.1 CEA-852 Gerät

Jeder L-IP arbeitet als Client-Gerät am IP-Kanal. Jeder Client muss entweder den Konfigurationsserver kontaktieren, oder der Konfigurationsserver muss den Client kontaktieren, um die richtigen IP-Routingtabellen zu setzen. Bevor ein Gerät Mitglied am CN/IP-Kanal werden kann, muss es folgende Parameter gesetzt haben:

- IP-Adresse/Netmask/Gateway (entweder über DHCP oder durch manuelle Eingabe, siehe Abschnitt 7.3.3)
- NAT-Adresse, wenn das Gerät hinter einer Firewall oder NAT-Router betrieben wird (automatisch erkannt mit Auto-NAT, siehe Abschnitt 7.3.12)
- MD5-Secret falls Authentifizierung gewünscht ist (siehe Abschnitt 7.3.12).

Bitte konsultieren Sie die Abschnitte 7.3.3 und 7.3.12 für detaillierte Instruktionen wie das CN/IP-Gerät zu initialisieren ist.

8.2.2 CEA-852 Konfigurationsserver

Jedes CEA-709 Gerät, das direkt auf einen IP-852 Kanal verbunden ist (Intranet, Internet) muss durch einen sogenannten Konfigurationsserver verwaltet werden (siehe Abbildung 94). Ein Konfigurationsserver überwacht eine Liste aller Geräte auf einem logischen IP-852 Kanal und verteilt die Routing-Information an all diese Geräte. Will ein Gerät am IP-852 Kanal teilhaben, muss es sich selbst im Konfigurationsserver registrieren.

Der L-IP kann mit seinem eingebauten Konfigurationsserver betrieben werden oder auch mit dem PC-basierenden *i*.LON Configuration Server Utility. Der eingebaute Konfigurationsserver kann im CEA-852-Server-Konfigurationsmenü des L-IP freigeschaltet werden, siehe Abschnitt 7.3.14. Dieser Konfigurationsserver kann einen IP-852 Kanal und bis zu 256 Geräte auf diesem IP-852-Kanal verwalten. Um den Konfigurationsserver richtig einzustellen müssen folgende Parameter gesetzt werden:

- IP-Adresse/Netzmaske/Gateway (entweder mit DHCP oder durch einen Eintrag), siehe Abschnitt 7.6.1

- NAT-Adresse, wenn das Gerät hinter einer Firewall/NAT-Router liegt, siehe Abschnitt 7.3.12
- MD5-Schlüsselwort, wenn mit Authentifizierung gearbeitet wird, siehe Abschnitt 7.3.12
- Freischalten des Konfigurationsservers, siehe Abschnitt 7.3.14 (Server-LED leuchtet dann grün)
- Mitgliederliste des IP-852-Kanals, siehe Abschnitt 7.3.15.

Hinweis: *Wird der L-IP auch als Konfigurationsserver verwendet, so muss er über eine fixe (öffentliche) IP-Adresse verfügen.*

Prinzipiell gibt es zwei Szenarios, wie ein Gerät in einen IP-852 Kanal aufgenommen werden kann. Entweder wurde in das Gerät eine gültige IP-Adresse eines Konfigurationsservers eingegeben und es kontaktiert den Konfigurationsserver selbst direkt, oder der Konfigurationsserver hat eine Liste der IP-Adressen der neuen Geräte und er kontaktiert die jeweiligen Geräte.

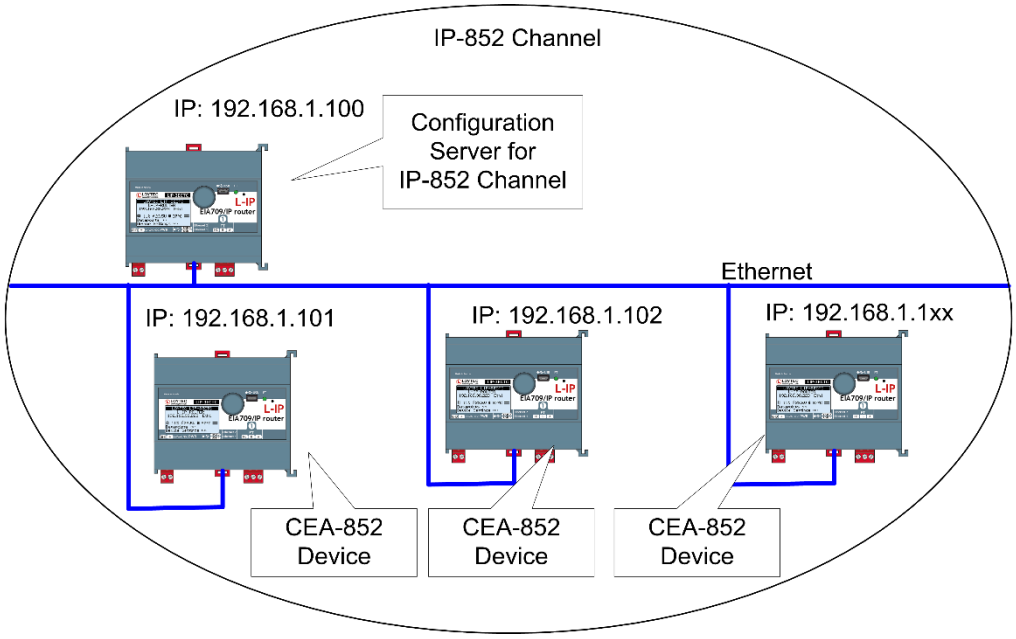


Abbildung 94: Der Konfigurationsserver verwaltet Geräte eines IP-852-Kanals.

8.2.2.1 Konfigurationsserver verbindet sich mit einem IP-852-Gerät

In diesem Szenario benötigt ein IP-852-Gerät folgende Parameter, damit ein Konfigurationsserver sich mit dem Gerät verbindet. Alle übrigen Parameter werden aus dem Konfigurationsserver gewonnen.

- IP-Adresse/Netzmaske/Gateway (entweder über DHCP oder durch einen Eintrag), siehe Abschnitt 7.3.3
- Auto-NAT oder manuelle NAT-Adresse, wenn hinter einer Firewall/NAT-Router gearbeitet wird, siehe Abschnitt 7.3.12
- MD5-Schlüsselwort, wenn mit einer Authentifizierung gearbeitet wird, siehe Abschnitt 7.3.12

Werden mehrere IP-852-Geräte, die hinter einem NAT-Router liegen, hinzugefügt, wird empfohlen, die Auto-NAT-Einstellung des L-IP mit Konfigurationsserver zu verwenden.

Hinweis: *Wird der L-IP auch als Konfigurationsserver verwendet, so muss er über eine fixe (öffentliche) IP-Adresse verfügen.*

8.2.2.2 IP-852-Gerät verbindet sich mit dem Konfigurationsserver

In diesem Szenario benötigt ein IP-852-Gerät folgende Parameter, damit sie sich zu einem Konfigurationsserver verbindet. Alle übrigen Parameter werden aus dem Konfigurationsserver gewonnen.

- IP-Adresse/Netzmaske/Gateway (entweder mit DHCP oder durch einen Eintrag), siehe Abschnitt 7.3.3
- Auto-NAT oder manuelle NAT-Adresse, wenn hinter einer Firewall/NAT-Router gearbeitet wird, siehe Abschnitt 7.3.12
- MD5-Schlüsselwort, wenn mit einer Authentifizierung gearbeitet wird, siehe Abschnitt 7.3.12
- IP-Adresse und Portnummer des Konfigurationsservers, siehe Abschnitt 7.3.12.

Wenn die Eigenschaft „Auto Member“ im Konfigurationsserver gesetzt wurde, kann das IP-852-Gerät sich selbst an den IP-852-Kanal hängen, ohne dass dies explizit durch einen Konfigurationsserver geschieht. Beachten Sie jedoch, dass diese Eigenschaft „Auto Member“ eine potenzielle Sicherheitslücke darstellt, denn dadurch kann sich jedes Gerät selbst an den IP-852-Kanal hängen.

8.2.2.3 Verwendung des integrierten Konfigurationsservers

Aus Sicherheitsgründen nimmt der Konfigurationsserver Verbindung mit jedem IP-852-Gerät auf dem IP-852-Kanal auf. Deshalb muss man eine Liste von Kanalmitgliedern in das CEA-852-Konfigurationsservermenü eintragen, siehe Abschnitt 7.3.15. Dies stellt sicher, dass keine ungewollten Geräte sich auf den IP-852-Kanal anmelden.

Auch Netzwerkknoten, die auf *i*.LON 1000/600, VNI und LOYTEC NIC852 basieren, können auf einen IP-852-Kanal durch den Konfigurationsserver verwaltet werden. Beachten Sie, dass der integrierte Konfigurationsserver verwendet werden muss, wenn LOYTEC CEA-852 Geräte über eine Firewall/NAT-Router kommunizieren sollen.

Zum Hinzufügen mehrerer Geräte, die hinter einem NAT-Router liegen, unterstützt der Konfigurationsserver den erweiterten (extended) NAT-Modus (siehe Abschnitt 8.3.2). Der Konfigurationsserver schaltet auf den erweiterten NAT-Modus, sollte dieser von Nöten sein. Beachten Sie, dass der *i*.LON 600 mit dem *i*.LON CS auf erweiterten (extended) NAT-Modus konfiguriert werden muss, noch bevor der *i*.LON 600 in den Konfigurationsserver eingetragen wird, weil der *i*.LON 600 nicht automatisch in diesen Modus schalten kann.

8.2.2.4 Verwendung des i.LON Konfigurationsservers

Der L-IP kann auch mit dem *i*.LON Configuration Server Utility verwendet werden. Wenn die L-IPs über eine Firewall/NAT-Router kommunizieren oder wenn MD5 Authentifizierung auf dem L-IP eingeschaltet ist, muss das *i*.LON Configuration Server Utility in der Version 2.00.24 oder höher verwendet werden. Der Kanalmodus des Konfigurationsserver muss dann auf “Standard CEA-852” gestellt sein. Beachten Sie bitte, dass dieser Modus den *i*.LON 1000 und LNS 3.0 VNI nicht unterstützt. Jedoch können LNS 3.0 Anwendungen (z.B. LonMaker) MD5 Authentifizierung und die NAT-Fähigkeit im Standard Mode verwenden, wenn der LOYTEC NIC852 Treiber verwendet wird.

Das *i*.LON Configuration Server Utility in der Version 2.00.24 und höher unterstützt ebenfalls den erweiterten (extended) NAT Modus (siehe Abschnitt 8.3.2), um mehr als ein Gerät hinter einem NAT Router zu betreiben. Der L-IP kann mit dem *i*.LON Configuration Server Utility in diesem Modus verwendet werden. Beachten Sie jedoch, dass der

Kanalmodus im *i*.LON Konfigurationsserver manuell auf “Extended NAT” Modus umgestellt werden muss.

Hinweis: *Wird der L-IP hinter einem NAT Router mit dem* i.*LON Konfigurationsserver verwendet, muss die Auto-NAT Funktion im L-IP abgeschaltet werden und die korrekte NAT-Adresse manuell eingegeben werden.*

8.3 Firewall und NAT Router Konfiguration

Der L-IP kann hinter einer Firewall bzw. einem NAT (Network Address Translation) Router, wie in Abbildung 95 dargestellt, betrieben werden. In Firmware-Versionen vor 3.0 kann nur maximal ***ein*** L-IP hinter einem NAT-Router betrieben werden. Dieser Modus wird als „Standard“ Channel-Modus bezeichnet und ist zu CEA-852 vollkommen kompatibel.

L-IPs mit Firmware-Versionen ab 3.0 unterstützen auch den Betrieb von mehreren L-IPs hinter einem NAT-Router. Dieser Modus wird als „Extended NAT“ Channel-Modus bezeichnet. In diesem Modus werden Erweiterungen verwendet, die mit Geräten früherer Firmware-Versionen nicht vollkommen kompatibel sind. Dazu zählen unter anderem der L-IP bis 2.2 und der *i*.LON 1000. Abschnitt 8.2.2.3 enthält weitere Informationen zur Kompatibilität mit dem *i*.LON 600.

8.3.1 Automatische NAT-Konfiguration

Um den L-IP hinter einer Firewall betreiben zu können, muss die öffentliche IP-Adresse des NAT-Routers sowie die private IP-Adresse des L-IP im IP Configuration Menu (siehe Abschnitt 7.3.3) gesetzt werden. In der Standardeinstellung wird die NAT-Adresse vom L-IP automatisch ermittelt, sobald der L-IP in einem L-IP Configuration Server einem Kanal hinzugefügt wird. (Auto-NAT).

Alternativ kann die NAT-Adresse auch manuell eingestellt werden. Als weiteren Schritt muss der NAT-Router so konfiguriert werden, dass die Ports 1628 und 1629 für UDP und TCP Pakete an die private IP-Adresse des L-IP (192.168.1.100 in Abbildung 95) weitergeleitet werden (Port-Forwarding). Zusammenfassend kann gesagt werden, dass folgende Parameter gesetzt werden müssen, um einen L-IP hinter einem NAT-Router betreiben zu können:

- Setzen der IP-Adresse (private IP-Adresse: z.B. 192.168.1.100),
- Setzen der Gateway-Adresse (z.B. 192.168.1.1),
- Setzen der NAT-Adresse (öffentliche IP-Adresse: z.B. 135.23.2.1) oder aktivieren der automatischen NAT-Router Erkennung,
- Einschalten des Port-Forwarding für die Ports 1628 und 1629 im NAT-Router für TCP und UDP,
- Aktivieren des SNTP-Port 123 in der Firewall, wenn SNTP verwendet wird (Internetverbindungen).

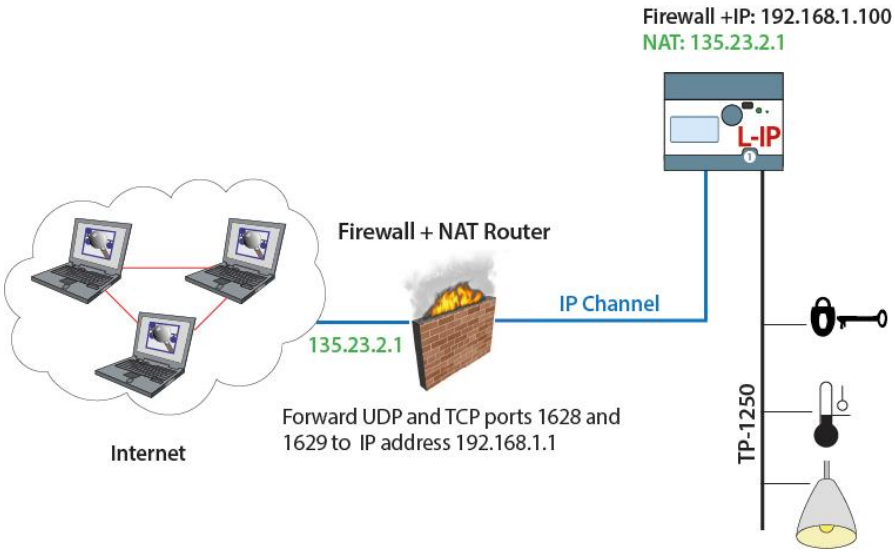


Abbildung 95: Betrieb eines L-IP hinter einem NAT-Router und Firewall.

Bitte beachten Sie, dass nur ein L-IP-Konfigurationsserver verwendet werden kann, wenn ein L-IP hinter einer Firewall oder NAT-Router betrieben werden sollte. In diesem Fall kann auch der L-IP, der als Konfigurationsserver agiert, hinter der Firewall und NAT-Router sitzen.

8.3.2 Mehrere L-IPs hinter einem NAT-Router: Extended NAT Modus

Wenn mehrere L-IPs hinter einem NAT-Router benutzt werden sollen, ist ab der Firmware-Version 3.0 der erweiterte (extended) NAT-Modus die empfohlene Methode. Dieser Modus setzt allerdings voraus, dass alle Geräte im IP-852 Kanal diesen Modus unterstützen. Derzeit sind das der L-IP 3.0, *i*.LON 600 und die NIC852 PC Software von LOYTEC. Falls andere Geräte am Kanal sind, die diesen Modus nicht unterstützen, funktioniert der Kanal nicht richtig. Inkompatible Geräte werden dann in diesem Kanal deaktiviert. Verwenden Sie in diesem Fall den klassischen Modus, wie in Abschnitt 8.3.3 beschrieben.

Beachten Sie, dass bei mehreren L-IPs hinter einem NAT-Router jeder L-IP sein eigenes Port Forwarding im NAT-Router eingetragen haben muss. Das setzt voraus, dass die Client-Portnummern unterschiedlich sind. Es wird empfohlen, den ersten L-IP auf Client Port 1628 zu belassen, den zweiten auf Client Port 1630, den dritten auf Client Port 1631, usw. einzustellen. Benützen Sie dazu das CEA-852 Device Configuration Menü in den L-IPs. Abbildung 96 zeigt ein Beispiel mit drei L-IPs hinter dem NAT-Router 135.23.2.1.

Es wird empfohlen, dass im NAT-Router das Port Forwarding für die Ports 1628 und 1629 auf dieselbe private Adresse eingestellt wird. Es ist dann auch möglich, den Configuration Server hinter dem NAT-Router zu betreiben. In diesem Fall sollte der CS auf dem L-IP eingeschaltet werden, wohin die Ports 1628 und 1629 weitergeleitet sind. Im Beispiel in Abbildung 96 kann der CS auf dem L-IP mit der privaten Adresse 192.168.1.100 eingeschaltet werden.

Es ist zu beachten, dass der NAT-Router, hinter dem ein L-IP mit Configuration Server betrieben wird, eine fixe öffentlich Adresse besitzen muss. Der L-IP mit dem CS kann außerdem keine automatische NAT-Konfiguration durchführen. Auf diesem L-IP muss die NAT-Adresse manuell eingestellt werden (Auto-NAT lässt sich nicht einschalten). Um mögliche Probleme in der NAT-Konfiguration zu diagnostizieren, wird der Enhanced Communications Test empfohlen (siehe Abschnitt 7.2.4).

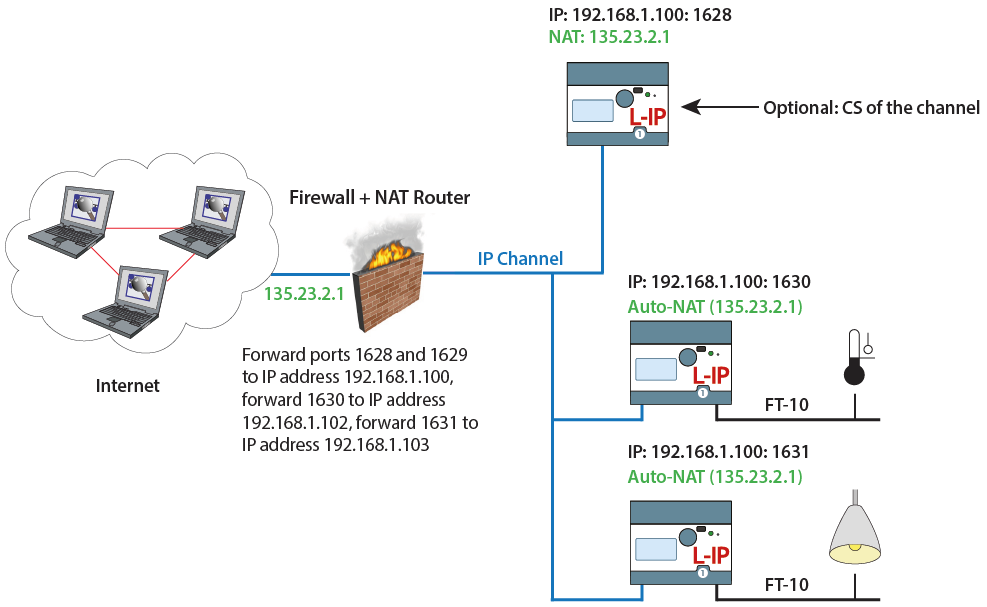


Abbildung 96: Mehrere L-IPs hinter einem NAT-Router: Extended NAT Methode

Nachdem der NAT-Router mit den entsprechenden Port-Forwardings konfiguriert und der CS aktiviert wurde, können die Geräte dem IP-852 Kanal hinzugefügt werden. Das kann sowohl über die Konsole als auch über das Web-Interface geschehen.

Im Web-Interface werden die einzelnen Teilnehmer mit ihren privaten IP-Adressen und Client-Ports, bezüglich ihrer Port-Forwarding-Definition, hinzugefügt. Dann wählen Sie die angefügten Teilnehmer mit Hilfe der Check-Box aus und aktivieren den Vorgang **Assign to NAT**. Geben Sie die öffentliche NAT-Adresse des NAT-Routers ein. Ein Beispiel wie zwei IP-852-Geräte der Abbildung 96 über das Web-Interface eingefügt werden, sehen Sie in Abbildung 97. Mit dem Aktionsfeld **Remove from NAT** kann ein Gerät aus dem NAT-Router entfernt werden, es wird dabei jedoch nicht gelöscht.

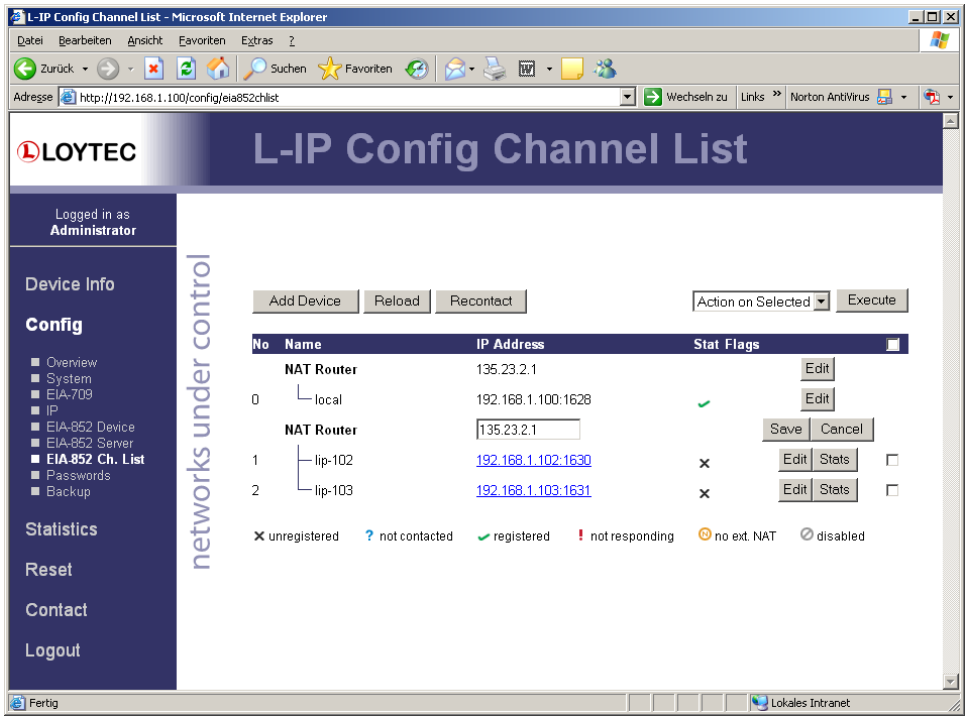


Abbildung 97: Hinzufügen eines Gerätes im Extended-NAT-Modus über das Web-Interface.

8.3.3 Mehrere L-IPs hinter einem NAT-Router: Klassische Methode

Sollte mehr als ein IP-852-Gerät hinter einem NAT-Router verwendet werden und es Geräte geben, die den Extended-NAT-Modus nicht unterstützen, so schlagen wir vor, den klassischen Aufbau wie in Abbildung 98 zu verwenden.

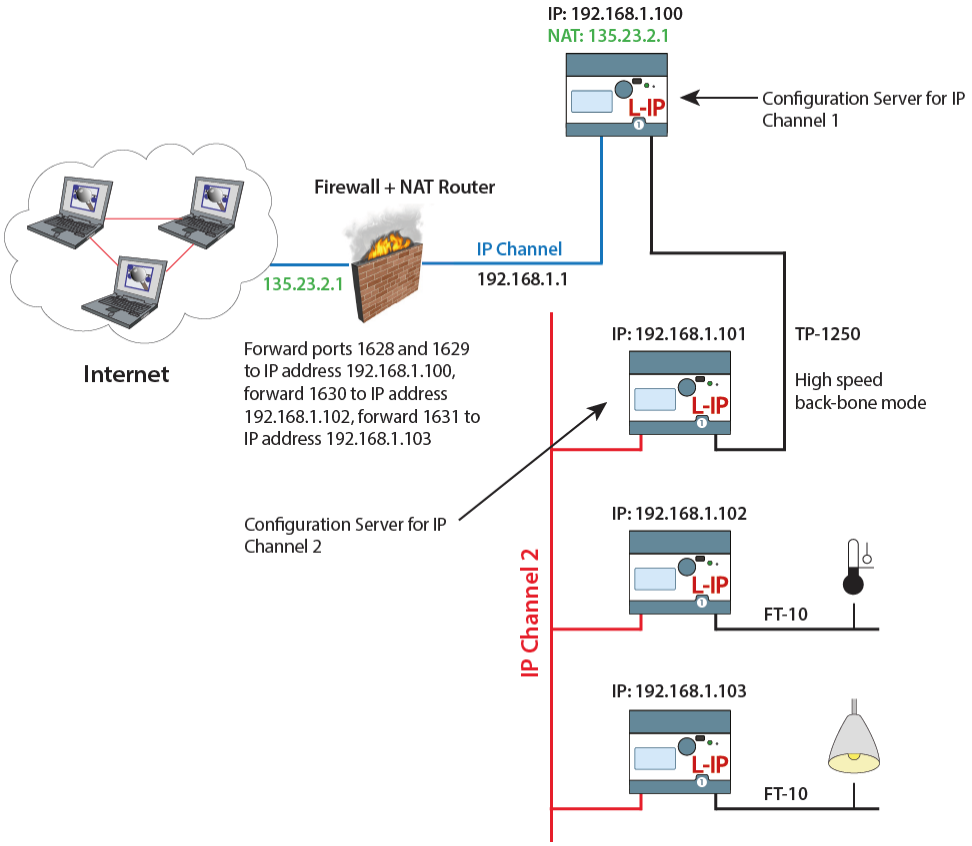


Abbildung 98: : Anwendung, die mehrere L-IP-Geräte hinter einer NAT-Router Firewall verwendet.

Der L-IP mit Adresse 192.168.1.100 ist Mitglied des IP Channel 1 und kann über das Internet erreicht werden. Die L-IPs mit Adressen 192.168.101 bis 192.168.1.110 bilden einen zweiten, logischen IP-852 Kanal mit Namen IP Channel 2. Der IP Channel 2 kommuniziert mit den Geräten am IP Channel 2 über den TP-1250 Kanal. Der TP-1250-Kanal wird im High-Speed-Backbonemodus betrieben, um eine möglichst geringe Verzögerungszeit für diese Verbindung zu gewährleisten. Bitte beachten Sie, dass selbstverständlich sowohl die Geräte am IP Channel 1 als auch am IP Channel 2 physikalisch mit dem selben Ethernet-Netzwerk verbunden werden können. Beide IP-852 Kanäle benötigen ihren eigenen Konfigurationsserver, der jeweils die Geräte auf IP Channel 1 bzw. auf IP Channel 2 verwaltet. In dem Beispiel in Abbildung 98 fungiert der L-IP mit Adresse 192.168.1.100 als Konfigurationsserver für den IP Channel 1 und der L-IP mit Adresse 192.168.1.101 als Konfigurationsserver für den IP Channel 2.

8.4 Multicast Konfiguration

IP-Multicast ist eine Technik, mit der ein IP-Paket gleichzeitig an eine Gruppe von IP-Knoten geschickt werden kann. Um solche Multicast-Pakete empfangen zu können, muss ein IP-Knoten in diese Gruppe konfiguriert werden. Die Gruppe wird dabei durch eine Multicast-Adresse (z.B. 225.0.0.37) und eine UDP-Portnummer identifiziert.

Seit der Firmware-Version 3.0 unterstützt der L-IP für das Senden von CN/IP-Datenpaketen sowohl normale (unicast) Pakete als auch die Multicast-Technik. Es wird empfohlen, die Multicast-Technik in L-IPs im Smart Switch Mode zu aktivieren. Dazu geben Sie bitte im IP Konfigurationsmenü eine Multicast-Adresse an. Kontaktieren Sie Ihren Systemadministrator, um eine gültige Multicast-Adresse für Ihr Netzwerk zu erhalten. Es ist zu beachten, dass alle L-IPs mit der gleichen Multicast-Adresse und dem selben Client-Port (z.B. 1628) konfiguriert werden müssen. Es sei auch darauf hingewiesen, dass die Multicast-Pakete nicht im Internet geroutet werden können. Daher kann diese Technik nur im Intranet (LAN oder VPN) eingesetzt werden.

Wenn die Multicast-Technik eingesetzt wird, kann es Geräte im Kanal geben, die kein Multicast unterstützen. In diesem Fall arbeitet der L-IP in hybrider weise und sendet Multicast-Pakete nur an jene Geräte, die sie unterstützen, sowie Unicast-Pakete an alle anderen Geräte. Um den gesamten Verkehrsaufwand zu optimieren, entscheidet der L-IP selbst, wann Multicast gesendet wird oder nicht. Als Daumenregel gilt, dass Multicast verwendet wird, wenn nur L-IPs im Smart Switch oder Repeater Mode vorhanden sind, und Unicast verwendet wird, wenn nur L-IPs im Configured Router Mode vorhanden sind.

Um festzustellen, ob ein L-IP nun die Multicast-Technik verwendet, um an andere Geräte zu senden, sehen Sie im Extended CEA-852 Device Statistics Menü nach (Abschnitt 7.2). Der Eintrag „Channel Routing Mode“ steht auf SL (send list), wenn der L-IP Multicast-Pakete versendet. Er steht auf CR (channel routing) wenn die herkömmliche Unicast-Technik verwendet wird. Außerdem zählt der Eintrag „Multi-cast packets sent“ im CEA-852 Device Statistics Menü (Abschnitt 7.2) die Anzahl der gesendeten Multicast-Pakete. Ist dieser Eintrag 0, wird vom L-IP kein Multicast verwendet.

8.5 Internet Timing Aspekte

Soll der CEA-709-Router über das Internet oder in einem großen Intranet mit unvorhersehbaren Zeitverzögerungen im Netzwerk kommunizieren, muss sich der Benutzer mit den folgenden erweiterten Zeitaspekten auseinander setzen. Der Parameter Channel-Timout wird im Konfigurationsserver eingestellt, wohingegen Escrowing und Aggregation im CEA-852-Client eingestellt werden. Die Channel-Delay ist eine Kanaleigenschaft des LNS und kann im NL220, LonMaker oder anderen Netzwerkmanagement-Tools eingestellt werden.

Tabelle 6 zeigt die Zeitparameter, die eingestellt werden müssen, wenn das Gerät in einem WAN betrieben werden soll.

Zeit-Parameter	Werte
Channel Timeout	Durchschnittliches Ping-Delay + Aggregation-Timeout
Escrowing (Packet Reorder Timer)	Der kleinere Wert aus 0.25*Channel-Timout oder 64 ms
Aggregation Timeout (Packet Bunching)	Typ. 16 ms
Channel Delay in LonMaker	Durchschnittliches Ping-Delay +10 % + 2* Aggregation-Timeout

Tabelle 6: Erweiterte IP-852-Zeitparameter.

Verwenden Sie einen PC zum Ermitteln der mittleren Verzögerungszeit von Ping-Nachrichten zwischen verschiedenen CEA-852 Geräten im Netzwerk. Kommunizieren mehrere Geräte miteinander, dann sollte immer die größte gemessene, mittlere Ping-Delay-Zeit für die Berechung der Tabelle 6 herangezogen werden.

Escrowing sollte in einer LAN-Umgebung deaktiviert (0 ms) werden. Die „Channel-Delay in LonMaker“ sollte auf 2*Aggregation-Timeout bei einer LAN-Umgebung eingestellt werden, falls MD5 deaktiviert ist.

Channel-Timeout ist in LAN-Umgebungen nur dann zu aktivieren, wenn MD5-Authentifizierung eingeschaltet ist. Setzen Sie in diesem Fall das Channel-Timeout auf 200 ms und das Channel-Delay auf 20 ms.

8.5.1 Channel-Timeout

Das Channel-Timeout ist eine Eigenschaft des IP-852-Kanals. Ist die Verzögerung eines Pakets auf dem IP-852-Kanal größer als der Wert, der im Channel-Timeout angegeben ist, so wird das Paket verworfen. Das Gerät muss sich mit einem SNTP-Zeitserver synchronisieren, wenn ein Channel-Timeout ungleich 0 ms eingestellt ist.

Es wird dringend empfohlen, das Channel-Timeout bei Betrieb mit MD5-Authentifizierung einzuschalten, um Replay-Angriffe (Angriff durch Wiedereinspielung) am Kanal zu verhindern. In einer LAN-Umgebung sollte der Channel-Timeout auf 200 ms und die Channel-Delay auf 20 ms eingestellt werden. Im Abschnitt 7.3.14 wird erklärt, wie sie die Channel-Timeout ein- oder ausschalten.

Wird eine LNS-basierendes Netzwerkmanagementsoftware wie z.B. LonMaker oder NL220 auf einem Netzwerk verwendet, das die Channel-Timeout aktiviert hat, so muss auf diesem PC ein NTP-Clientprogramm (z.B. achron4.exe) installiert werden, um die PC-Zeit mit der Uhr des CEA-852-Geräts zu synchronisieren. Ansonsten könnte die PC-Uhr und die Uhr des CEA-852-Geräts auseinanderdriften und die Kommunikation zwischen PC und dem Gerät beenden.

8.5.2 Channel-Delay

Das Channel Delay ist eine LNS-Kanaleigenschaft, die die erwartete Umlaufzeit einer Nachricht und Ihrer Antwort angibt. Dieser Wert wird von LNS verwendet, um die Protokolltimer in den CEA-709-Knoten anzupassen. Bitte sehen Sie im Handbuch Ihrer Netzwerkmanagementsoftware zum Thema Channel-Delay nach.

8.5.3 Escrowing-Timer (Packet-Reorder-Timer)

Der Escrowing-Timer (oder auch Packet-Reorder-Timer) ist eine IP-852-Kanaleigenschaft, die angibt, wie lange ein Gerät auf ein IP-Paket zuwartet, das nicht in der richtigen Reihenfolge übertragen wurde. Dieser Parameter ist in WAN-Netzen wie dem Internet von Bedeutung, wo Pakete über unterschiedliche Routen geschickt werden und somit die Reihenfolge der am Zielknoten eintreffenden IP-Pakete verändern können. Der Standardwert sind 64 ms.

Verwenden Sie den Escrowing-Timer nicht in LAN-Umgebungen, wo die Paketreihenfolge immer garantiert wird. Dies würde zusätzliche, unnotwendige Verzögerungen in der Paketübertragung bewirken, die sich negativ auf die Leistungsfähigkeit der CEA-852-Geräte auswirken, falls ein Paket verloren geht.

Egal ob ein- oder ausgeschaltet Pakete, die nicht der Paketreihenfolge entsprechen, werden nicht auf den CEA-709-Kanal weitergeleitet. Bitte lesen Sie Abschnitt 7.3.12 zum Ein- und Ausschalten des Escrowing-Timers.

8.5.4 SNTP-Zeitserver

Kleine IP-Netzwerke wie z.B. LANs haben typischerweise kurze Verzögerungszeiten um Datenpakete zu übertragen. In diesen Netzwerken ist es nicht notwendig SNTP-Server anzugeben.

In großen IP-852-Netzwerken wie z.B. das Internet, wo lange Paketverzögerungszeiten auftreten können, muss man einen SNTP-Server einbauen, damit sich die Uhren der CEA-852-Geräte synchronisieren können. Die lokalen Uhren müssen sich auf eine gemeinsame Zeitbasis synchronisieren, damit die CEA-852-Protokollfunktionen wie z.B. das Escrowing und Channel Timeout richtig funktionieren.

Der SNTP-Zeitserver wird im Konfigurationsserver als Eigenschaft des IP-852-Kanals angegeben. Der Konfigurationsserver verteilt dann die Zeitserver-Adresse an alle CEA-852-Geräte auf dem IP-852-Kanal. Es kann ein primärer und ein sekundärer SNTP-Server definiert werden. Wie ein SNTP-Server aktiviert wird sehen Sie im Abschnitt 7.3.12 und 7.3.14.

8.6 Erweiterte Themen

8.6.1 Aggregation

Aggregation (oder auch Paketbündelung genannt) ist eine Technik, die mehrere CEA-709-Pakete in ein einzelnes, größeres IP-Paket zusammenfassen kann. Aggregation verbessert die Leistungsfähigkeit Ihres Gesamtsystems, da ein IP-Paket mehrere CEA-709-Pakete transportieren kann und somit mit der gleichen Anzahl von IP-Transaktionen mehrere CEA-709-Pakete zwischen den CEA-852-Geräten ausgetauscht werden können. Dies reduziert den Protokoll-Overhead auf der IP-Seite. Der Aggregation-Timeout-Parameter definiert die Zeitperiode in ms, in der das absendende Gerät die CEA-709-Pakete zusammenfasst, bevor es ein IP-852-Paket am IP-852-Kanal aussendet. Abschnitt 7.3.12 zeigt, wie Aggregation ein- und ausgeschaltet werden kann. Bitte beachten Sie, dass Aggregation eine kurze Verzögerung zur Transaktionszeit hinzufügt, jedoch mittels Aggregation ein viel höherer Paketdurchsatz am IP-852-Kanal erreicht wird. Verwenden Sie Aggregation, wenn Sie eine hohe Kanalbelastung haben und die im Aggregation Zeitwert angegebene zusätzliche Verzögerung tolerieren können.

8.6.2 MD5-Authentifizierung

MD5-Authentifizierung ist eine Methode, um die Authentizität einer Nachricht zu verifizieren. Nur Geräte, die MD5-Authentifizierung aktiviert haben und das gleiche MD5-Schlüsselwort (Secret) verwenden, können Datenpakete austauschen. Wenn der Konfigurationsserver MD5 aktiviert hat, können sich nur IP-852-Geräte auf diesem IP-852-Kanal anmelden, die ebenfalls MD5 aktiviert haben und das gleiche MD5-Schlüsselwort wie der Konfigurationsserver verwenden. Abschnitte 7.3.12 und 7.3.14 geben Auskunft über die Verwendung von MD5.

8.6.3 DHCP

Wenn DHCP verwendet wird, muss sichergestellt werden, dass der Konfigurationsserver immer dieselbe IP-Adresse zugewiesen bekommt. Client-Geräte hingegen können auch unterschiedliche IP-Adressen bekommen, solange die Funktion “Roaming Member” auf dem Konfigurationsserver aktiviert ist. Verwenden Sie kein DHCP mit dynamischen IP-Adressen in Anwendungen mit NAT-Routern.

8.6.4 Dynamische NAT-Adressen

Bei Internet-Providern ist es durchaus üblich, dem Kunden IP-Adressen mit jedem Verbindungsaufbau neu zuzuweisen. Jedes Mal, wenn eine Verbindung aufgebaut wird (z.B. ein ADSL-Link) wählt der Internet-Provider eine IP-Adresse aus seinem Pool aus. Da diese IP-Adresse normalerweise die öffentliche Adresse des NAT-Routers ist, müsste das CEA-852-Gerät nach jedem Verbindungsaufbau neu konfiguriert werden. Die Auto-NAT-Funktion kann daher die IP-Adresse des NAT-Routers während des Betriebes beobachten. Falls eine Änderung bemerkt wird, registriert sich das CEA-852-Gerät beim Konfigurationsserver mit der neuen NAT-Adresse. Diese Funktion benötigt jedoch einen LOYTEC Konfigurationsserver (z.B. L-INX, L-IP) und die Eigenschaft „Roaming Members“ muss in diesem CS aktiviert sein.

Das Beobachten der NAT-Adresse hat jene Auswirkung, dass das CEA-852 Gerät alle 45 Sekunden den CS kontaktiert, um die NAT-Adresse zu testen. Dies produziert ein bisschen zusätzlichen Verkehr auf der Internet-Verbindung. Die Auto-NAT-Funktion fungiert außerdem als „Keep-Alive“ für die Verbindung. Dies hat zur Folge, dass eine Internet-Verbindung automatisch wieder aufgebaut wird. Ist weder der zusätzliche Verkehr noch der automatische

Verbindungsaufbau tolerierbar, dann muss die Auto-NAT-Funktion abgeschaltet und die NAT-Adresse manuell eingestellt werden. In diesem Fall muss der Internet-Provider dem NAT-Router eine fixe IP-Adresse zuweisen.

8.7 Netzwerk-Buffer

Der L-IP kann Pakete vom Netzwerk mit einer maximalen Länge von 256 Bytes verarbeiten. Es gibt keine explizite Limitierung in der Anzahl an Netzwerk-Buffern.

9 Der L-IP im Netzwerk

Der L-IP basiert auf der leistungsfähigen L-Core™ and L-Chip™ Technologie von LOYTEC. Er ist für einen robusten und zuverlässigen Betrieb entwickelt worden und zeichnet sich durch eine einfache Installation aus. Der L-IP verhält sich entweder vollkommen transparent im Netzwerk oder kann als konfigurierter CEA-709-Router eingesetzt werden.

Bevor der L-IP mit dem Routen von Datenpaketen beginnen kann, muss er einem CN/IP-Kanal hinzugefügt werden. Bitte konsultieren Sie Abschnitt 8.2.2 für Instruktionen, wie der L-IP einem CN/IP-Kanal hinzugefügt werden kann.

9.1 L-IP agiert als Standard CEA-709 Configured Router

Die Installation und der Betrieb des L-IP ist wie bei einem Standard CEA-709 Router. Dies ist die Betriebsart des L-IP mit Werkseinstellungen:

- Konfigurierter CEA-709-Router,
- Bitratenerkennung eingeschaltet, und
- Backbone-Modus für TP-1250-Port ausgeschaltet.

Nachdem der L-IP einem CN/IP-Kanal hinzugefügt wurde, muss der L-IP mit einem Netzwerkmanagement-Tool wie z. B. NL-220 von Newron Systems oder LonMaker von Echelon in das Projekt eingefügt und kommissioniert werden. LOYTEC stellt LonMaker Shapes für den L-IP zur Verfügung, die von unserer Website geladen werden können: http://www.loytec.com/deutsch/download/lip.htm.

Der Multiport-L-IP enthält mehrere Standard-CEA-709-Router, wobei jeder dieser Router einem der Ports zugeordnet ist und die Router über einen internen TP-1250 Kanal verbunden sind. Der interne TP-1250 Kanal ist nach außen hin weder sichtbar noch kann er angesprochen werden. Seine einzige Aufgabe ist es, die internen Router untereinander zu verbinden. Abbildung 99 zeigt ein Beispiel für den Multiport-L-IP (LIP-33ECTB).

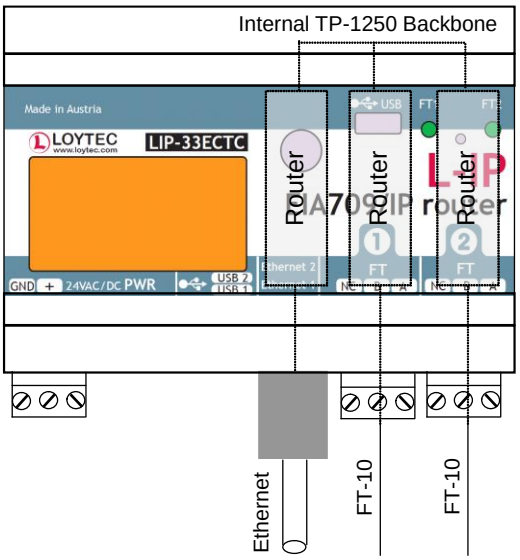


Abbildung 99: Interne Struktur des Multiport-L-IP im CEA-709 Router-Modus

Jeder der internen Router muss separat kommissioniert werden, wobei die Struktur mit dem internen TP-1250 Kanal in der Kommissionierung beachtet werden muss. Die Port-LEDs unkonfigurierter Ports blinken mit einer Frequenz von 1 Hz (einmal pro Sekunde).

Um den Port auszuwählen auf dem eine „Service Pin Message“ Nachricht ausgesendet werden soll, muss der Statustaster länger als 2 Sekunden gedrückt gehalten werden. Die Port-LED des gerade selektierten Ports leuchtet orange auf. Wird der Statustaster weiter gedrückt gehalten, so wird nach weiteren 2 Sekunden der nächste Port selektiert. Sobald der Statustaster freigegeben wird, wird von dem momentan selektierten Port/Router eine „Service Pin Message“ Nachricht ausgesendet.

Die Application Note AN003G „L-IP und LNS“ enthält detaillierte Hinweise für die Installation eines Multiport-L-IP mit einem LNS basierenden Netzwerkmanagement-Tool (z.B.: LonMaker).

9.2 L-IP agiert als Smart Switch

Wird der L-IP als Switching Router („Smart Switch Modus“) verwendet, so ist die Installation und Inbetriebnahme Plug&Play. Der Smart Switch Modus kann mittels der DIP-Schalter eingestellt werden (siehe Abschnitt 8.1.2). Nach Anschluss der Netzwerkkabel und der Stromversorgung startet der L-IP seine Switch-Applikation. Bevor der L-IP zu routen beginnen kann, muss er noch in einen CN/IP-Kanal hinzugefügt werden.

Mit einem Netzwerkmanagement-Tool können Bindings zwischen Knoten, die sich auf unterschiedlichen Ports des L-IP befinden, gemacht werden, ohne dass der L-IP beachtet werden muss. Der L-IP kann in dieser Betriebsart auch in bereits bestehende Anlagen installiert werden, ohne das Netzwerk umkonfigurieren zu müssen.

In dieser Plug&Play-Betriebsart unterstützt der L-IP keine CEA-709-Router Netzwerkmanagement Kommandos. Jedoch unterstützt er alle anderen Standard-Netzwerkmanagementkommandos (z. B. um die Kanalparameter zu setzen).

9.3 L-IP agiert als L-Switch

Bestehende Installationen, die nur TP-1250- und/oder FT-10-Segmente verwenden, können Router zwischen den Netzwerksegmenten erfordern. In diesem Fall ist weder ein IP-852-

Kanal noch sind irgendwelche IP-Einstellungen erforderlich. In solchen Installationen wurden die älteren LOYTEC L-Switch™-Geräte verwendet. Andere Hersteller stellten ebenfalls LON-Router zur Verfügung (z. B. Echelon LonPoint™-Router).

Der L-IP mit zwei Ports kann als Gerät vom Typ L-Switch konfiguriert werden. In diesem Modus ist der IP-852-Kanal deaktiviert und der interne Router fungiert als Smart Switch™ oder als konfigurierter CEA-709-Router zwischen seinen TP-1250- und/oder FT-10-Ports. Ein Beispiel für einen LIP-33ECTC, der als Gerät vom Typ L-Switch konfiguriert ist, finden Sie in Abbildung 100.

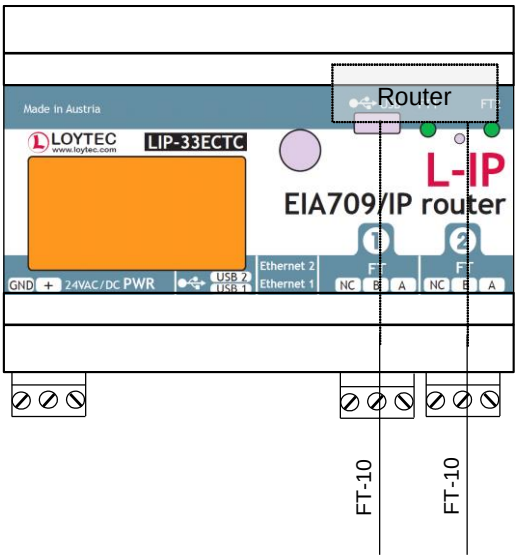


Abbildung 100: Interne Struktur eines Zweiport-L-IP konfiguriert als L-Switch.

9.4 Verwendung des L-IP in LNS (LonMaker) Netzwerken

Wir stellen LonMaker Shapes für den L-IP zur Verfügung, wenn der L-IP in LonMaker-Projekten verwendet werden soll. Es können selbstverständlich auch die normalen Routershapes verwendet werden. Bitte laden Sie die Shapes von unserer Website http://www.loytec.com/deutsch/download/lip.htm.

Detaillierte Informationen, wie der L-IP gemeinsam mit LNS-basierenden Netzwerkmanagement-Tools verwendet werden kann, finden Sie in Kapitel 15.

9.5 L-IP als Netzwerkinterface für LNS Anwendungen

Der L-IP kann als lokales oder Remote-Netzwerkinterface für LNS-basierende Applikationen wie z.B. LonMaker verwendet werden, um auf das CEA-709-Netzwerk zuzugreifen. Dazu muss das CEA-852-Netzwerkinterface auf dem PC, auf dem die LNS-Applikation gestartet wird, konfiguriert werden und die IP-Adresse des PCs bei dem Konfigurationsserver für den CN/IP-Kanal registriert werden.

1. Fügen Sie die IP-Adresse des PC's in die Geräteliste am Konfigurationsserver hinzu (siehe Abschnitt 7.3.15).

2. Starten Sie das LonWorks Interfaces Applet aus der Systemsteuerung und wählen Sie den Reiter **IP-852**.

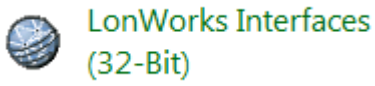


Abbildung 101: Icon für LonWorks Interfaces in der Windows 7 Systemsteuerung.

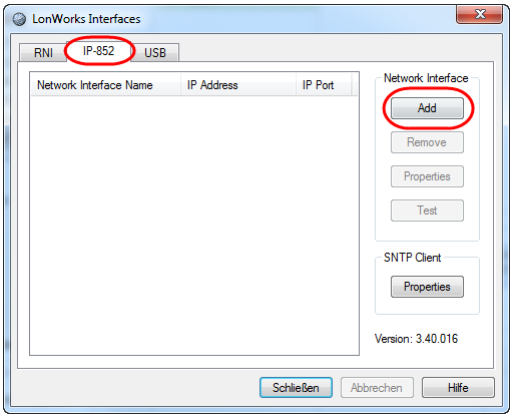


Abbildung 102: Hinzufügen eines neuen LNS IP Interface am PC.

3. Klicken Sie auf **Add** und geben Sie einen **Namen** für das neue Interface ein. Das Feld **IP Address** zeigt die IP-Adresse Ihres PC's an. Belassen Sie den IP-Port auf 1628 und das Feld MD5 Authentication Key leer. Klicken Sie dann **OK**.

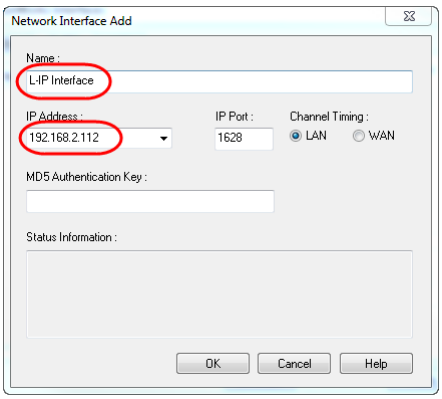


Abbildung 103: Geben Sie den neuen Interfacenamen ein.

4. Klicken Sie auf **Properties** im SNTP Client Bereich. Schalten Sie den SNTP Client nicht ein, wenn das Netzwerkinterface in einem lokalen Netzwerk (z.B. einem Intranet) betrieben wird. Wird auf das Netzwerkinterface auch über ein großes Netzwerk wie dem Internet zugegriffen, sollten Sie die Adressen für Time Server eingeben und den SNTP Client einschalten. Falls Sie aber bereits einen anderen NTP-Client auf dem PC installiert haben, der die Uhr des PC's mit einem NTP Timer Server synchronisiert, dürfen Sie den SNTP-Client nicht auch noch einschalten, sonst würde dieser mit dem bereits installierten NTP-Client auf dem PC konkurrieren.

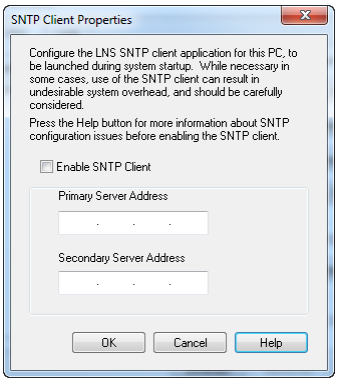


Abbildung 104: Deaktivieren Sie den SNTP-Client falls Sie einen lokalen NTP-Client auf dem PC installiert haben.

5. Nun können Sie die LNS-Anwendung starten und das “L-IP Interface” als Ihr Interface zum CEA-709-Netzwerk auswählen.

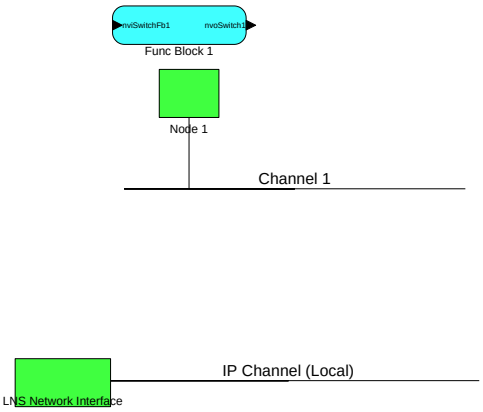


Abbildung 105: Verbinden Sie das LNS-Network-Interface mit dem neu erzeugten “IP Channel”

6. Wird der L-IP als ein CEA-709 Configured Router verwendet, sollten Sie den L-IP in die LonMaker Zeichenfläche hinzufügen. Erzeugen Sie dazu einen neuen Channel mit dem Typ ‚IP-10L’ für ein Intranet oder ‚IP-10W’ für eine Internet-Umgebung. Ändern Sie das LNS Netzwerkinterface auf diesen neu erzeugten IP-Kanal, wie in Abbildung 105 gezeigt. Wählen Sie dazu das LNS Netzwerkinterface aus, und wählen Sie den Punkt **Change Channel** aus dem Kontext-Menü.

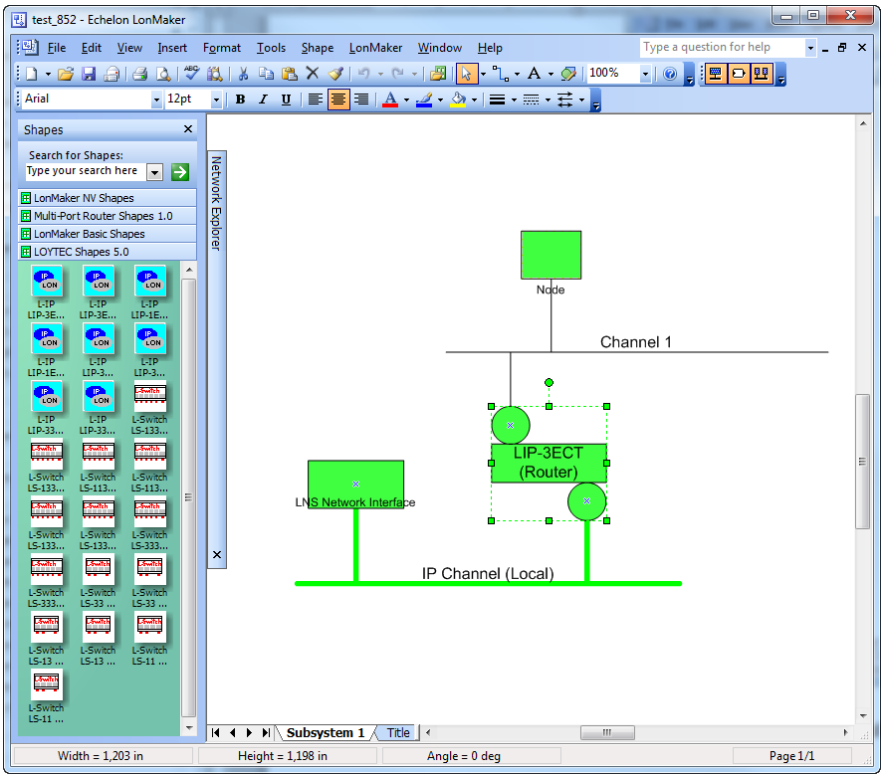


Abbildung 106: Ziehen Sie das L-IP (Router) Shape auf die Zeichenfläche und kommissionieren Sie den L-IP.

7. Nun ziehen Sie das L-IP (Router) Shape aus den “LOYTEC Shapes” auf die Zeichenfläche. Wählen Sie den existierenden Kanal “IP Channel” für den ersten Router-Port und den existierenden Kanal “Channel 1” für den zweiten Port. Zuletzt müssen Sie noch den neuen L-IP Router kommissionieren. LonMaker kann nun den L-IP als ein lokales oder Remote-Netzwerkinterface verwenden, das direkt mit dem Ethernet-Netzwerk verbunden ist, wie in Abbildung 106 gezeigt.

9.6 Remote-LPA Betrieb

Beginnend mit Firmwareversion 2.0 unterstützt der L-IP den Remote-LPA Zugriff. Remote-LPA Betrieb bedeutet, dass ein Protokollanalysator, der an das Ethernet Netzwerk angeschlossen ist, sich mit dem L-IP verbinden kann und alle Pakete am lokalen CEA-709 Kanal (FT-10 oder TP-1250) aufzeichnen kann. Der LPA-IP unterstützt diese wichtige Funktionalität. Die prinzipielle Funktionsweise ist in Abbildung 107 dargestellt.

Der LPA-IP wird auf einem Windows PC ausgeführt, der an das Ethernet Netzwerk angeschlossen ist. In einem L-IP Auswahlfenster des LPA-IP kann der gewünschte L-IP z.B. mit der IP-Adresse 192.168.1.210 ausgewählt werden. Der LPA-IP kann nun sämtliche Datenpakete des lokalen FT-10 Kanals dieses L-IP darstellen. Um diese Funktion auszuführen muss der LPA-IP nicht Mitglied am CN/IP-Kanal sein. Bitte beachten Sie, dass diese Funktionalität nur mit L-IP Internet Routern zur Verfügung steht.

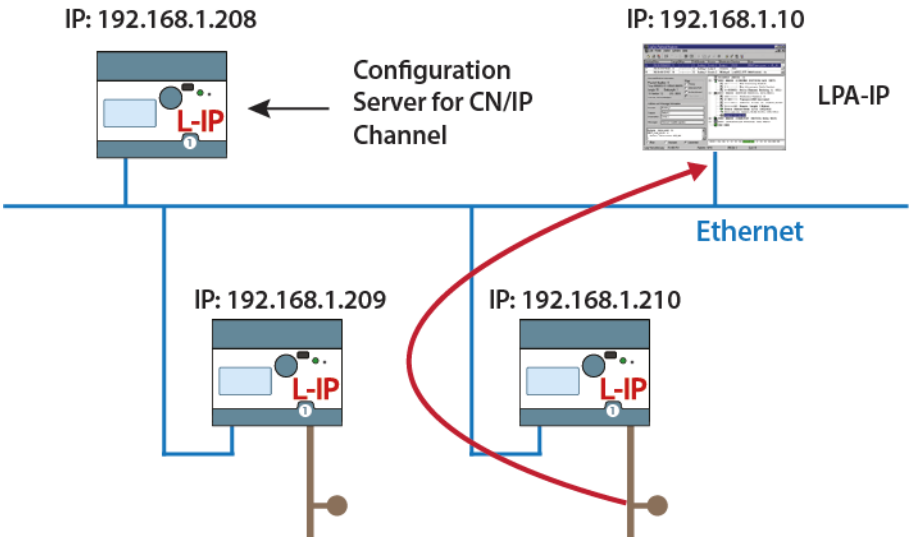


Abbildung 107: Remote-LPA Funktionsweise.

10 L-IP Redundant

10.1 Redundanz und Fehlererkennung in CEA-709 Netzwerken

10.1.1 Ursachen für Kommunikationsfehler

Abbildung 108 zeigt typische Ursachen für Kommunikationsprobleme in CEA-709 Netzwerken:

1. **Verbindungsfehler auf dem Backbone**: Der Router ist nicht mehr an den Backbone angebunden. Daher können die Knoten auf dem an den Router angeschlossenen Kanal nicht mehr mit Knoten auf anderen Kanälen oder der Gebäudeleitstation kommunizieren (A).

2. **Routerausfall**: Der Router fällt auf Grund eines Stromversorgungsfehlers oder Gerätegebrechens aus. Auch hier ist eine Kommunikation der Knoten auf dem an den Router angeschlossenen Kanal mit Knoten auf anderen Kanälen oder der Gebäudeleitstation nicht mehr möglich (A,B).

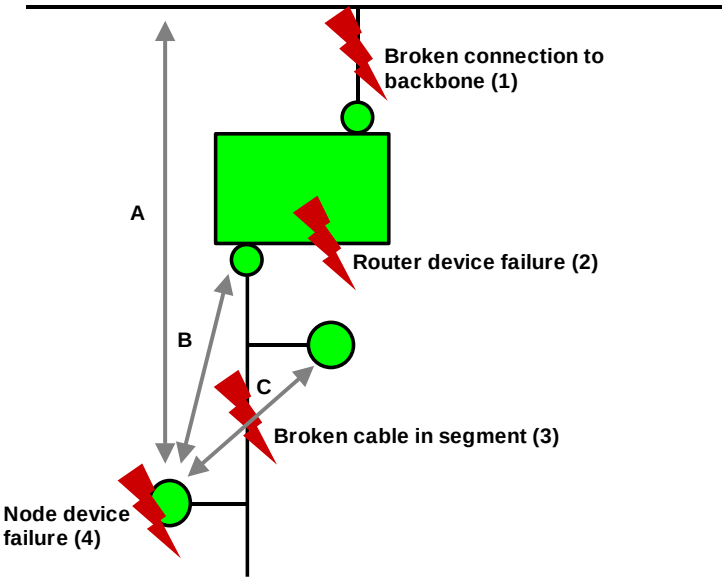


Abbildung 108: Typische Ursachen für Kommunikationsprobleme in CEA-709 Netzwerken

3. **Kabelbruch in einem Kanal**: Die Knoten können nicht über das gebrochene Kabel hinweg kommunizieren. Daher ist die Kommunikation von Knoten hinter dem Kabelbruch mit jenen vor dem Kabelbruch (C), dem Router (B) und mit Knoten in anderen Segmenten (A) nicht möglich.

4. **Knotenausfall**: Ein Knoten fällt auf Grund einer fehlerhaften Stromversorgung oder eines Knotendefekts aus. Daher kann der Knoten seine Funktion nicht mehr erfüllen und mit seinen Kommunikationspartner kommunizieren (A,B,C).

10.1.2 Herkömmliche Strategien zur Redundanz in CEA-709 Netzwerken

Der CEA-709.1 Standard erlaubt den redundanten Aufbau von Netzwerken mit Hilfe von herkömmlichen CEA-709.1 Routern (Twin Router), die in einem Netzwerk parallel und mit identischer Konfiguration eingesetzt werden. Dieser Ansatz hat jedoch 2 Nachteile. Zum einen wird der Netzwerkverkehr durch die zweifache Weiterleitung der Pakete wesentlich erhöht, was wiederum zu Kommunikationsproblemen führen kann. Zum anderen können damit nur die Problemkreise 2 (Routerausfall) und bis zu einem gewissen Grad Problem 1 (Verbindungsfehler auf dem Backbone)[1] vermieden werden.

Der Einsatz von herkömmlichen CEA-709/IP Routern zusammen mit einer redundanten IP Infrastruktur erlaubt die Behebung von Problem 1 (Verbindungsfehler auf dem Backbone), die Anbindung der Router (Kabel, Ethernet Switch) bleibt jedoch eine mögliche Fehlerursache („single point of failure“).

10.2 L-IP Redundant Betriebsarten

10.2.1 Bus Loop Monitoring

Um das Problem 3 (Kabelbruch in einem Kanal) zu vermeiden (siehe Abschnitt 10.1.1), erlaubt der L-IP Redundant eine ringförmige Verkabelung („Loop“), wobei die beiden Enden des Ringes mit den beiden Anschlüssen des Geräts verbunden werden (siehe Abbildung 109).

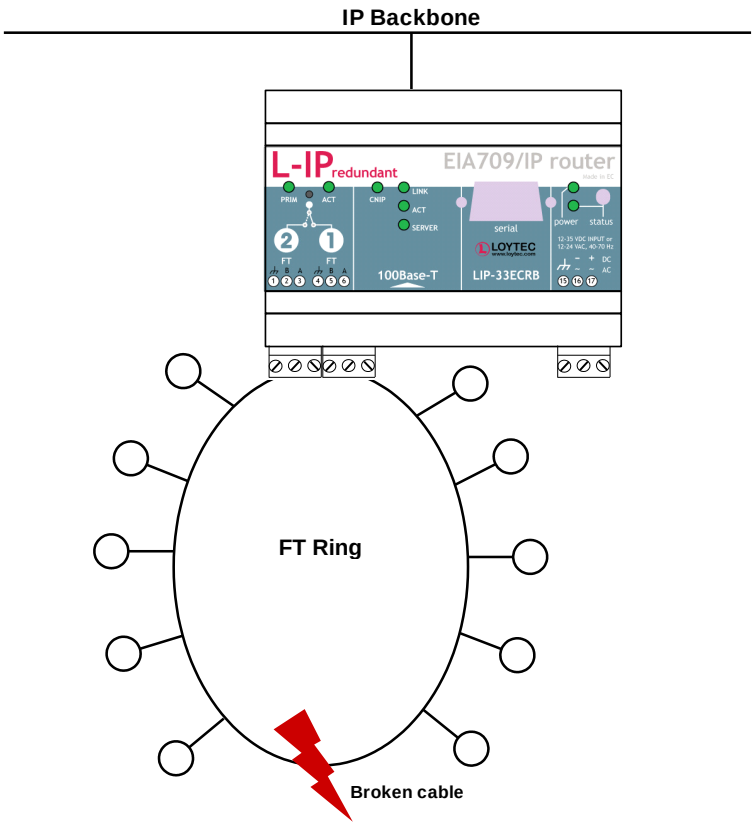


Abbildung 109: L-IP Redundant mit Bus Loop Monitoring

Nun kann der L-IP Redundant einen Kabelbruch erkennen, indem er ständig der Verkehr auf beiden Seiten des Buskabels vergleicht. Wenn an den beiden Enden ein unterschiedliches

[1] Unter der Voraussetzung, dass der Backbone redundant ausgeführt ist.

Verkehrsaufkommen erkannt wird, so wird ein Kabelbruch angenommen. In diesem Fall wird der Verkehr von Port 1 auf Port 2 bzw. umgekehrt dupliziert. Des weiteren wird ein Alarm generiert (siehe Abschnitt 10.5.5 und 10.6.3). Werden die Nachrichten wieder auf beiden Seiten empfangen, so wird angenommen, dass die Unterbrechung behoben wurde.

In der Werkseinstellung des L-IP Redundant ist das Bus Loop Monitoring aktiviert. Ist die Bus Loop Überwachung nicht erwünscht so muss sie deaktiviert werden um einen permanenten „Loop Open“ Alarm zu vermeiden. Die Bus Loop Monitoring Parameter können über das L-IP Redundant Plug-In (siehe Abschnitt 10.5.7) oder das Web Interface eingestellt werden (siehe Abschnitt 10.6.5).

Der aktuelle Bus Loop Monitoring Status kann über Netzwerk Variable (siehe Abschnitt 10.7), im L-IP Redundant Plug-In (siehe Abschnitt 10.5.3), und im Web Interface (siehe Abschnitt 10.6.1) angezeigt werden.

Wichtig:	***Für eine zuverlässige Funktion des Bus Loop Monitoring Algorithmus ist es erforderlich, die durchschnittliche Kanalauslastung unter 50% zu halten! Die Bandbreitenauslastung kann mit dem LOYTEC LPA oder über die eingebauten Diagnosefunktionen ermittelt werde (siehe Abschnitte 10.5.4 und 10.6.1).***

10.2.2 Router Redundanz

Wenn ein redundantes IP Netzwerk zur Verfügung steht, so kann volle Redundanz auf dem IP Backbone Kanal durch parallele Installation von zwei Routern erreicht werden (siehe Abbildung 110). In diesem Fall wird Routerredundanz durch gegenseitige Überwachung der beiden Router erreicht. Da zwei Router in gleicher Konfiguration eingesetzt werden, wird dieser Modus auch „Twin Router“ Modus genannt.

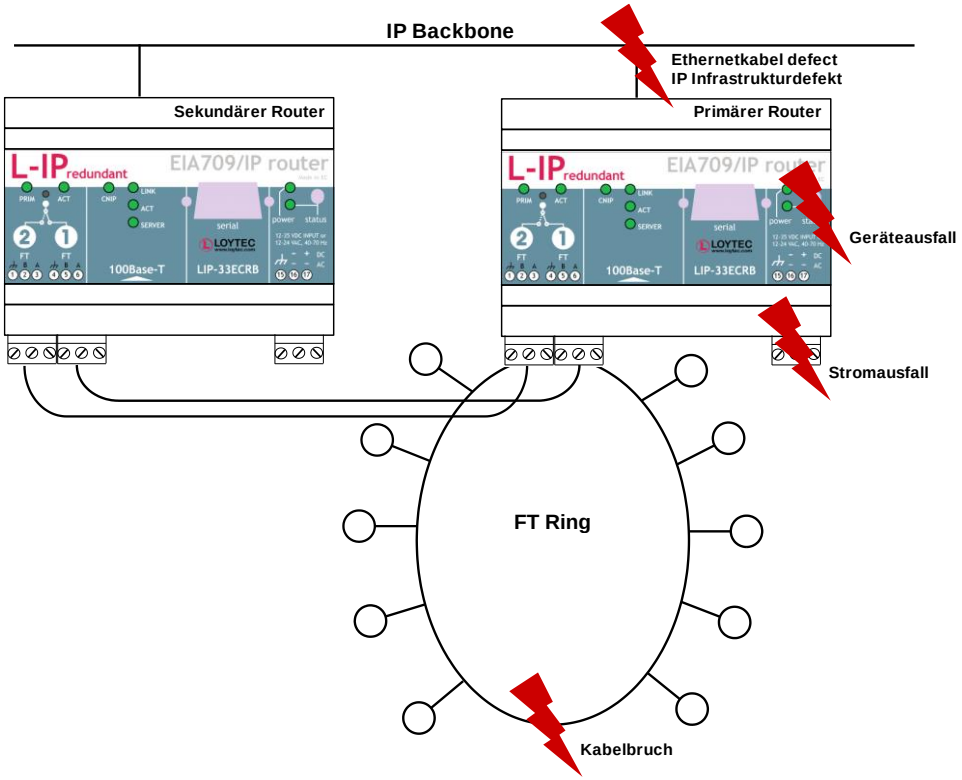


Abbildung 110: Router Redundanz durch paarweise eingesetzte L-IP Redundant Router

Während der Startphase wird zwischen den beiden L-IP Redundant Router automatisch ausgehandelt, welches Geräte die Funktion des primären Routers („Primary Router“) und welcher die des sekundären, inaktiven Geräts („Secondary Router“ bzw. „Standby Router“)

einnimmt[2]. Der aktive, primäre Router übernimmt das Routing der Pakete, die Schleifennüberwachung („Bus Loop Monitoring“) und die Knotenüberwachung („Node Monitoring“). Der inaktive Router hat diese Funktionen deaktiviert. Nach der Startphase überwachen sich die Router gegenseitig sowohl auf den CEA-709 Kanal als auch auf dem CEA-852 Kanal. Erreicht der sekundäre Router den primären Router auf einem der beiden Kanäle nicht mehr, so übernimmt er die Aufgabe des primären Routers und setzt einen Alarm ab. Erreicht der primäre Router den sekundären Router nicht, so wird lediglich ein Alarm ausgesendet.

Während der sekundäre Router inaktiv ist, leitet er keine Pakete weiter. Dennoch läuft der Routingalgorithmus normal ab und die Pakete, die basierend auf den Routingtabellen weitergeleitet *würden*, werden gezählt. Die ermittelten Zahlen werden periodisch zwischen primären und sekundären Router ausgetauscht und verglichen. Weichen die Zahlen signifikant voneinander ab, so wird ein Alarm abgesetzt. Dieser Algorithmus stellt sicher, dass die Routingtabellen beider Router konsistent sind und der sekundäre Router im Fehlerfall die Rolle des primären Routers übernehmen kann. Leitet der primäre Router keine Pakete weiter und wird festgestellt, dass der sekundäre Router Pakete weiterleiten würde, so übernimmt der sekundäre Router die Rolle des primären Routers und der primäre Router wird inaktiv.

Redundante Router können mit oder ohne Bus Loop Monitoring verwendet werden (siehe Abschnitt 10.2.1).

Um redundante Router zu betreiben müssen beide Router kommissioniert und an denselben CEA-852 Kanal angebunden sein. Des Weiteren müssen die beiden Router über Netzwerkvariablen verbunden werden, die zur Kommunikation zwischen den Routern verwendet werden. Genaue Informationen zur Konfiguration des L-IP Redundant Routers in diesem Modus finden Sie in Abschnitt 10.4.3.2.

Die Parameter für den redundanten Routerbetrieb können über das L-IP Redundant Plug-In (siehe Abschnitt 10.5.7) oder das Web Interface (siehe Abschnitt 10.6.5) konfiguriert werden.

Der aktuelle Zustand des Routers kann über Netzwerkvariable (siehe Abschnitt 10.7), im L-IP Redundant Plug-In (siehe Abschnitt 10.5.3) und über das Web Interface (siehe Abschnitt 10.6.1) abgefragt werden.

10.2.3 Knoten- und Netzwerküberwachung

Neben den Redundanzfunktionen kann der L-IP Redundant auch eine Reihe von Überwachungsfunktionen durchführen. Einerseits wird eine Anzahl von Indikatoren für die Kanalqualität (z.B. Kanalauslastung, CRC-Fehlerrate, usw.) permanent überwacht und deren aktuelle Werte werden als Netzwerkvariablen (siehe Abschnitt 10.7), im L-IP Redundant Plug-In (siehe Abschnitt 10.5.4) und im Web Interface (siehe Abschnitt 10.6.1) zur Verfügung gestellt.

Der L-IP Redundant kann aber auch dazu verwendet werden, um bis zu 128 andere Knoten im Netzwerk zu überwachen. Zu diesem Zweck kann eine Liste der zu überwachenden Knoten im L-IP Redundant Plug-In (siehe Abschnitt 10.5.6) oder dem Web Interface (siehe Abschnitt 10.6.4) erstellt werden. Ist die Knotenüberwachung aktiviert, so kontaktiert der L-IP Redundant die ausgewählten Knoten periodisch mittels Query Status Netzwerkdiagnosekommandos. Wenn ein Knoten nicht erreichbar ist oder sich in einem „Offline“-Status befindet, so wird ein Alarm ausgesendet. Der aktuelle Zustand der Knoten kann auch über eine Netzwerkvariable (siehe Abschnitt 10.7), im L-IP Redundant Plug-In (siehe Abschnitt 10.5.3), und im Web Interface (siehe Abschnitt 10.6.1) abgefragt werden. Zusätzlich zeigt das Web Interface Statistikinformationen aus den Knoten an (z. B. Anzahl der CRC Fehler).

[2] Der primäre Router ist jener mit der höheren VID1.

Bei aktiviertem Bus Loop Monitoring (siehe Abschnitt 10.2.1) überprüft der L-IP Redundant auch, von welcher der beiden Seiten bzw. auf welcher der beiden Ports die Knoten erreichbar sind (beide Seiten, nur Seite 1, nur Seite 2). Wenn die Knoten in der korrekten, ihrer Position am Buskabel entsprechenden, Reihenfolge in die Knotenliste eingegeben wurden dann kann auf diese Weise auch die Position eines Kabelbruchs erkannt werden. Diese Information wird auch über Netzwerkvariablen, das L-IP Redundant Plug-In und über das Web Interface zur Verfügung gestellt.

10.3 Der L-IP Redundant im Netzwerk

Wie in Abbildung 111 gezeigt besteht der L-IP Redundant intern aus einem standard CEA-709 Router und einem Diagnoseknoten. Der Router leitet Pakete zwischen dem CEA-709 und dem CEA-852 Kanal weiter, während der Diagnoseknoten die Überwachungsfunktionen (z. B. Knotenüberwachung) übernimmt und die Resultate über Netzwerkvariable zur Verfügung stellt.

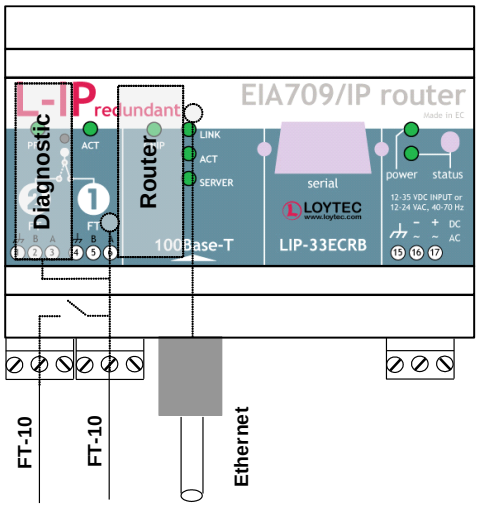


Abbildung 111: Interne Struktur des L-IP Redundant

Der Router im L-IP Redundant kann nur als Configured Router eingesetzt werden und muss daher mit einem Netzwerkmanagementwerkzeug kommissioniert werden. Ein Betrieb im Smart Switch Modus, Repeater oder Bridge Modus wird nicht unterstützt.

Da der Diagnoseknoten auf dem CEA-709 Kanal des Routers sitzt, muss der Router zuerst kommissioniert werden bevor von der CEA-852 Seite auf den Diagnoseknoten zugegriffen werden kann. Zur Konfiguration des Diagnoseknotens stell LOYTEC das L-IP Redundant Plug-In (siehe Abschnitt 10.4.1) bereit.

10.4 Installation

10.4.1 Installieren des L-IP Redundant Plug-In

Das L-IP Redundant Plug-In wird verwendet, um den Redundant Diagnoseknoten zu konfigurieren (siehe Abschnitt 10.2.3), die Parameter des L-IP Redundant einzustellen, die Alarmaufzeichnungen des L-IP Redundant herunterzuladen und um den aktuellen Status des L-IP Redundant anzuzeigen. Dieses Konfigurationsprogramm wird als LNS Plug-In installiert..

Systemanforderungen:

- LNS 3, Service Pack 7 oder höher
- Windows XP, Windows Vista oder Windows 7.

Das L-IP Redundant Plug-In kann von der LOYTEC Webseite (http://www.loytec.com) geladen werden.

Zur Installation der Plug-Ins führen Sie bitte folgende Schritte durch. Doppelklicken Sie auf die ausführbare Installationsdatei.



Abbildung 112: Stellen Sie sicher, dass sie unter Windows 2000/XP Administratorrechte haben.



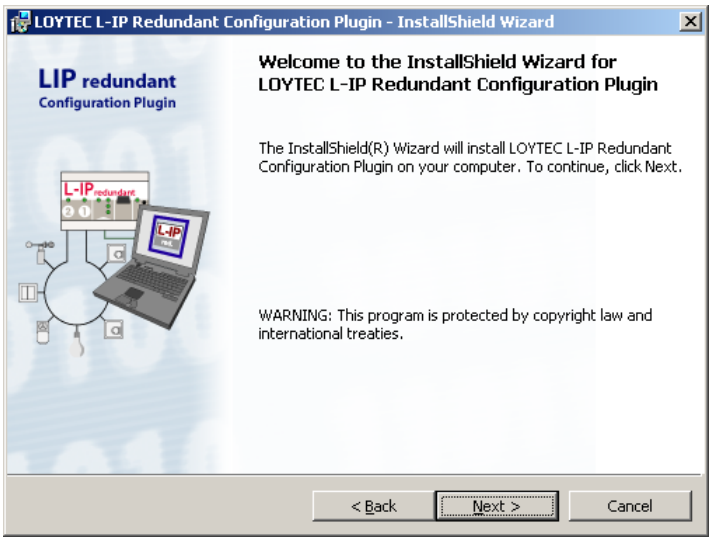


Abbildung 113: L-IP Redundant Plug-In Begrüßungsbildschirm

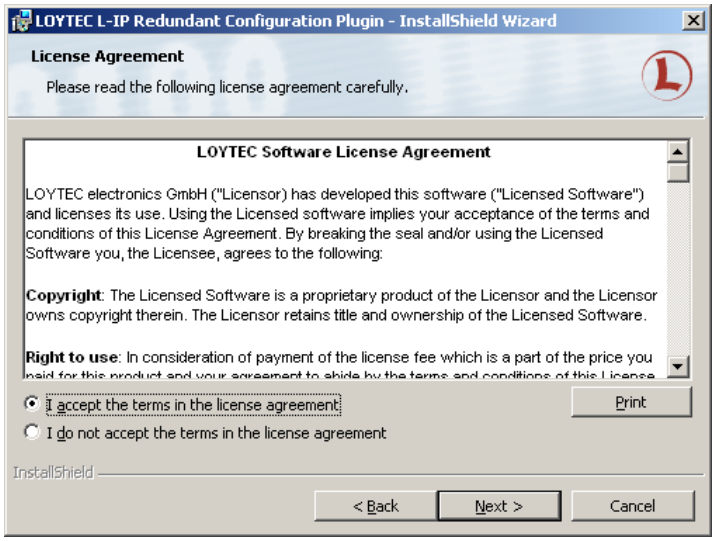


Abbildung 114: Sie müssen der Lizenzvereinbarung zustimmen

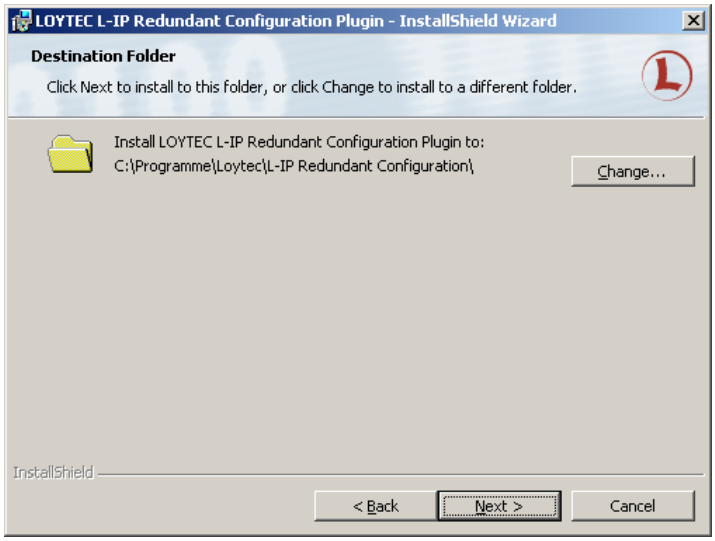


Abbildung 115: Wählen Sie das Zielverzeichnis aus

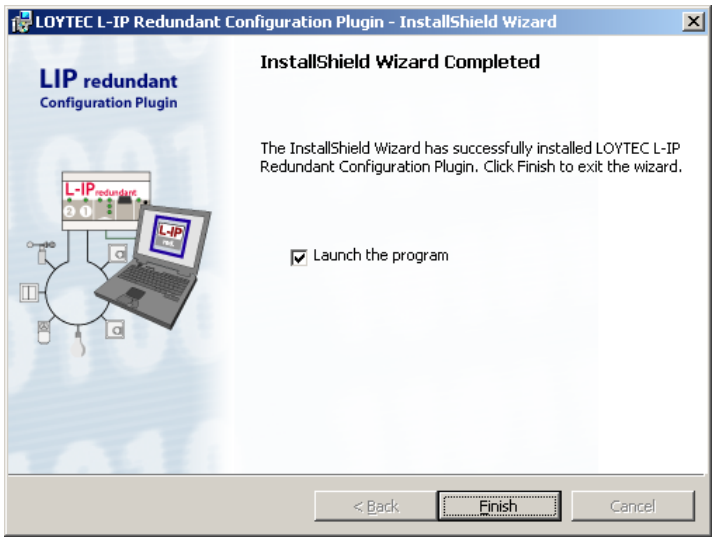


Abbildung 116: Das Plug-In wurde erfolgreich installiert

10.4.2 Registering des L-IP Redundant Plug-In

Nach der erfolgreichen Installation muss das Plug-In noch im LNS Projekt registriert werden. Die folgenden Schritte beschreiben diesen Vorgang in LonMaker for Windows 3.1. Folgen Sie der Dokumentation ihres Netzwerkmanagementprogramms zur Registrierung von Plug-Ins.

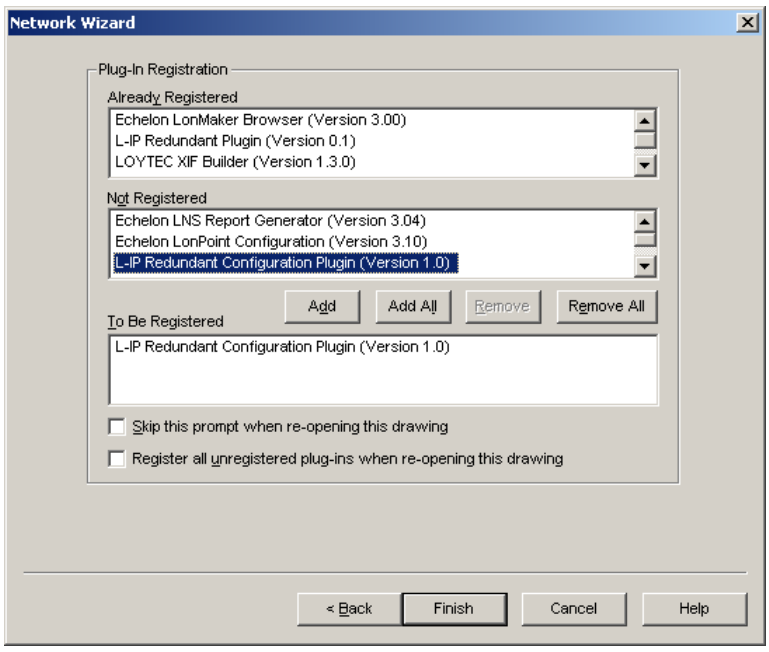


Abbildung 117: Wählen Sie das Plug-In aus und wählen Sie „Add“

Öffnen Sie LonMaker und erstellen Sie ein neues Netzwerk. Beim Erscheinen des Fensters „Plug-in Registration“ wählen Sie **L-IP Redundant Configuration Plug-In** aus der Liste „Not Registered Plug-Ins“ (siehe Abbildung 117). Wählen Sie „Add“ und „Finish“ aus um das Plug-In zu registrieren. Gerätevorlagen für den L-IP Redundant Diagnoseknoten werden automatisch hinzugefügt und die XIF Datei in das LNS Import Verzeichnis kopiert.

Hinweis:	*Wenn Sie mehrere Projekte verwenden stellen Sie sicher, dass das Plug-In in jedem Projekt registriert wird.*

In **LonMaker → Network Properties → Plug-In Registration** können sie überprüfen, ob das **L-IP Redundant Configuration Plug-In** korrekt registriert wurde und unter „Already Registered“ erscheint.

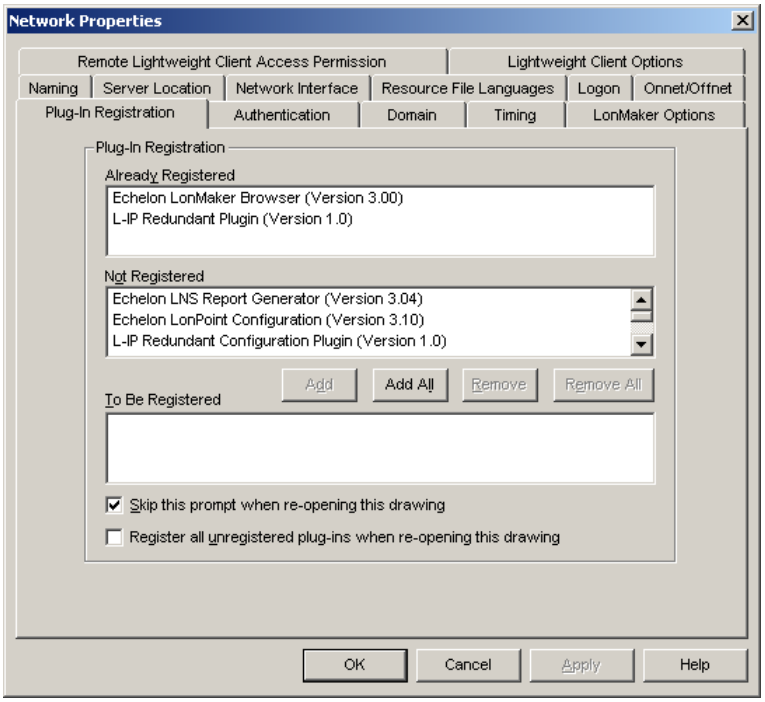


Abbildung 118: Überprüfen Sie, ob das L-IP Redundant Configuration Plug-In korrekt registriert wurde

10.4.3 Einfügen des L-IP Redundant

Der L-IP Redundant kann als Einzelgerät oder als redundanter Router eingesetzt werden. Abhängig vom Redundanzmodus sind unterschiedliche Schritte zur Konfiguration im Netzwerk erforderlich.

10.4.3.1 L-IP Redundant als Einzelgerät

Für den Einsatz als Einzelgerät sind folgende Schritte erforderlich:

- Fügen sie ein einzelnes Router Shape ein. Verbinden Sie den Router mit dem IP-Kanal und einem FT-10 Kanal.
- Fügen sie ein „L-IP Redundant Diagnostic FT-10“ Gerät auf dem FT-10 Kanal ein. Die zugehörige Gerätevorlage wurde bereits bei der Plug-In Installation angelegt. (siehe 10.4.1).

In LonMaker for Windows sollte das Ergebnis wie in Abbildung 119 aussehen.

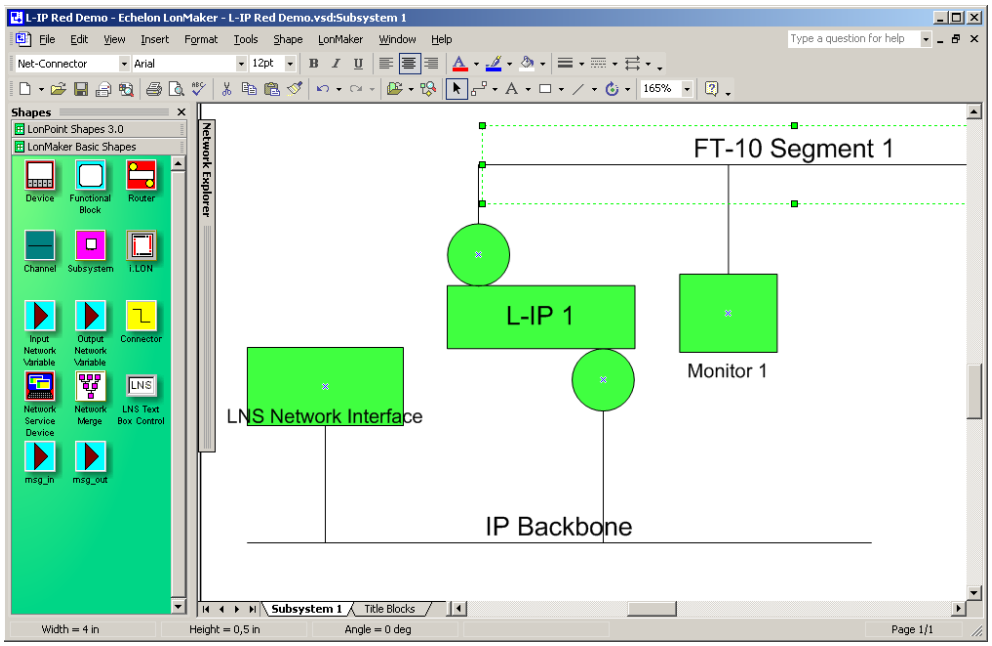


Abbildung 119: A Ein einzelner L-IP Redundant im Einzelgerätemodus

Kommissionieren sie den Router und den Diagnoseknoten. Nach erfolgreicher Einbindung muss die PRIM LED des Gerätes grün leuchten.

10.4.3.2 L-IP Redundant mit redundantem Router

Zum Betrieb des L-IP Redundant im Twin Router Modus (siehe Abbildung 110) sind folgende Konfigurationsschritte erforderlich:

- Fügen sie zwei Router Shapes ein. Verbinden sie jeweils den IP-Kanal und einen der beiden FT-Kanäle mit den Routern.

- Fügen Sie für jeden der beiden Router einen L-IP Redundant Diagnoseknoten „L-IP Redundant Diagnostic FT-10“ auf dem jeweiligen FT-10 Kanal ein. Die zugehörige Gerätevorlage wurde bei der Installation des L-IP Redundant Plug-Ins (siehe Abschnitt 10.4.1) erstellt.

- Fügen Sie zwei „Twin Router” Funktionsblöcke, jeweils einen für jeden L-IP Redundant, ein.

- Verbinden Sie die Netzwerkvariable *nvoRedRtr* des einen L-IP Redundant mit *nviRedRtr* des jeweils anderen L-IP Redundant und umgekehrt.

- Connect nvoRedRtr of one L-IP Redundant with the nviRedRtr of its paired L-IP Redundant and vice versa.

In LonMaker for Windows sollte das Ergebnis wie in Abbildung 120 dargestellt aussehen.

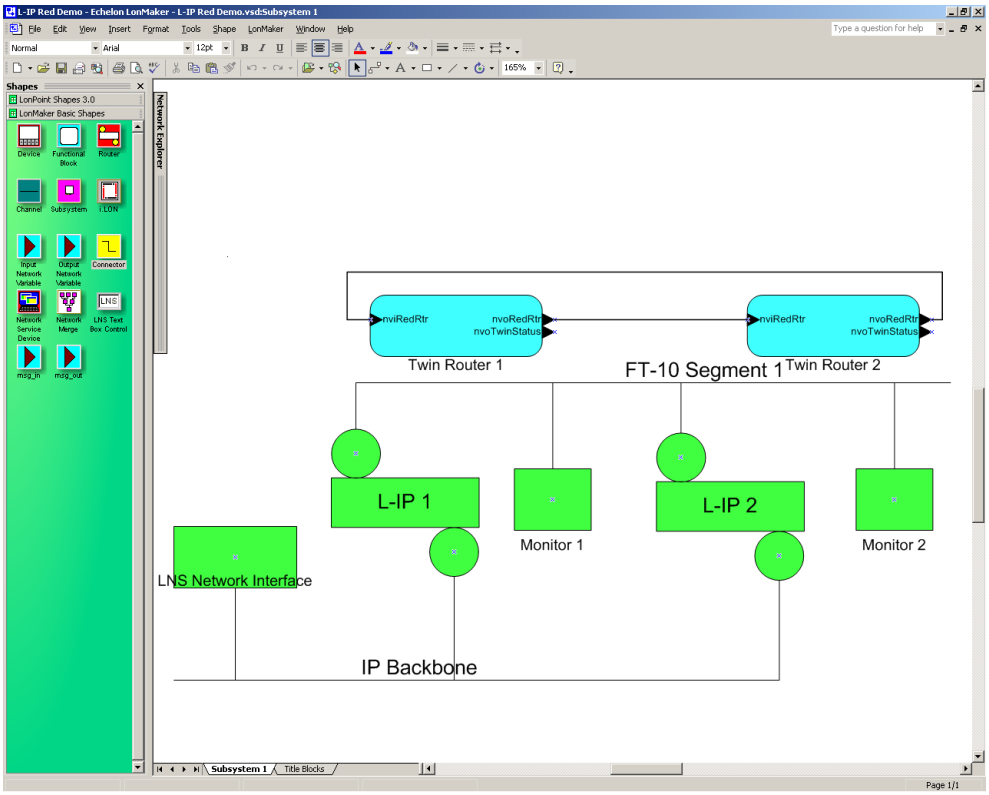


Abbildung 120: Ein Paar von L-IP Redundant Routern im redundanten Betrieb

Kommissionieren sie beide Router und beide Diagnoseknoten. Nachdem die Router und Diagnoseknoten erfolgreich kommissioniert wurden, muss die PRIM LED auf einem der L-IP Redundant Knoten grün leuchten und auf dem anderen L-IP Redundant Gerät ausgeschaltet sein.

Wichtig:	***Wenn Bus Loop Monitoring (siehe Abschnitt 10.2.1) nicht verwendet wird und der Port 2 Anschluss des L-IP Redundant Routers daher unbenutzt ist, dann muss zunächst ein L-IP Redundant und dessen Diagnoseknoten kommissioniert werden und das Bus Loop Monitoring ausgeschaltet werden bevor die Netzwerkvariabeln mit dem zweiten L-IP Redundant verbunden werden!***

Nachdem der Router und der Diagnoseknoten eingebunden worden ist, kann eine Knotenliste oder andere Parameter mit Hilfe des L-IP Redundant Plug-Ins (siehe Abschnitt 10.5) oder dem Web Interface (siehe Abschnitt 10.6) eingestellt werden.

10.5 L-IP Redundant Plug-In

10.5.1 Betriebsmodi

Das L-IP Redundant Configuration Plug-In kann online, offline oder standalone betrieben werden. Online und offline Modus bezieht sich auf die beiden Modi des Netzwerkmanagementprogramms.

10.5.1.1 Online Modus

Dies ist der bevorzugte Modus und erlaubt, die volle Funktionalität des Plug-Ins zu nutzen. Das Netzwerkmanagementprogramm ist mit dem Netzwerk verbunden und alle Änderungen werden direkt in die am Netzwerk angeschlossenen Knoten geschrieben. Dieser Modus ist erforderlich um Geräte zu kommissionieren, die Knotenliste in oder aus den Geräten zu

laden, die Alarmliste zu laden oder zu löschen und um den aktuellen Status des Gerätes abzufragen.

10.5.1.2 Offline mode

Im Offline Modus können alle Aufgaben, die LNS benötigen, durchgeführt werden. Geräte können mit Hilfe der Gerätevorlagen hinzugefügt werden, Geräteeigenschaften konfiguriert werden und die Knotenlist automatisch aus der LNS Datenbank generiert werden (LNS Import). Es ist jedoch keine Kommunikation mit den Geräte möglich (z. B. Laden der Knotenliste).

10.5.1.3 Standalone mode

Das L-IP Redundant Plug-In kann auch als eigenständiges Programm ausgeführt werden. In dieser Betriebsart steht jedoch nur ein eingeschränkter Funktionsumfang zur Verfügung. Es ist möglich, eine Knotenliste manuell zu generieren und eine Konfigurationsdatei zu laden, zu verändern und abzuspeichern.

10.5.2 Übersicht

Abbildung 121 zeigt das L-IP Redundant Configuration Plug-In. Das Hauptfenster ist in drei Bereiche geteilt:

- Der Anzeigeauswahl erlaubt, verschiedene Konfigurations- und Diagnoseseiten anzuzeigen.
- Abhängig vom der gewählten Anzeige werden im Anzeigebereich unterschiedliche Informationen angezeigt (z. B. Knotenliste).
- Das Log-Fenster zeigt alle durchgeführten Aktionen des Plug-Ins sowie Warnungen und Fehlermeldungen an.

Über die Toolbar können in Abhängigkeit von der ausgewählten Anzeige verschiedene Aktionen ausgewählt werden. Die Kommandos „Load“, „Save“ und „New“ können immer ausgewählt werden. Mit „Save“ kann die gesamte Konfiguration (Knotenliste, Einstellungen) und der Alarmlog in eine Datei gespeichert werden, während der „Lord“ Befehl diese Informationen aus einer Datei lädt. Die Informationen in der „L-IP Red. Status“ Ansicht und in der „Channel Statistics“ Ansicht werden nicht gespeichert.

Die „Twin Router“ Auswahl zeigt den Namen des primären und – wenn verfügbar – des sekundären Routers an. Der aktuell ausgewählte Router ist markiert. Durch Klicken kann auf den anderen Router umgeschaltet werden.

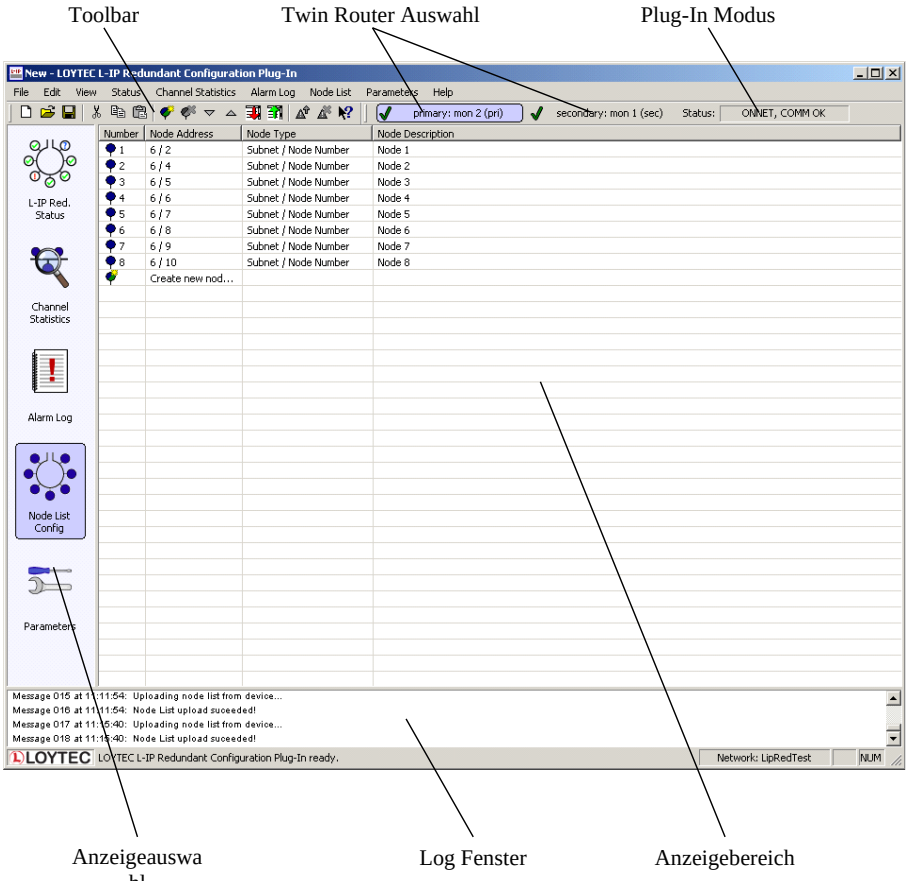


Abbildung 121: Das L-IP Redundant Konfigurations Plug-In

Der „Plug-In Modus“ zeigt den aktuellen Betriebsmodus (siehe Abschnitt 10.5.1) an.

10.5.3 Gerätestatus

Die Gerätestatusansicht („Device Status“) zeigt den aktuellen Zustand des L-IP Redundant an. Die Seite wird durch Anwahl der „L-IP Red. Status“ Schaltfläche im L-IP Redundant Plug-In angezeigt (siehe Abbildung 122).

Hinweis:	*Die meisten Statusinformationen sind nur im Online Modus, wenn auf das Geräte zugegriffen werden kann, verfügbar.*

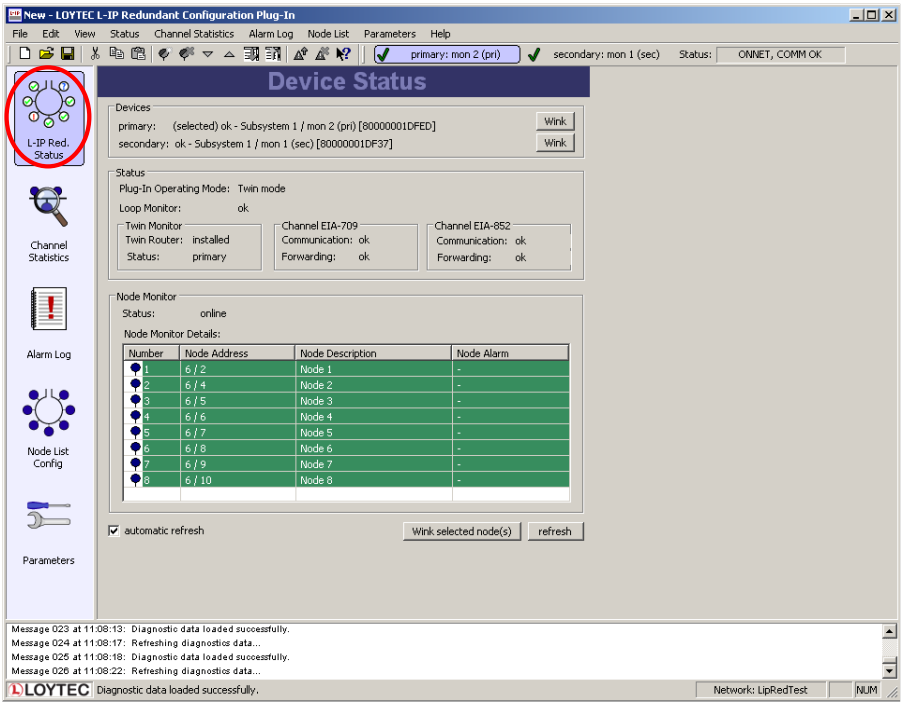


Abbildung 122: Der Gerätestatus

Die Gerätestatusansicht besteht aus folgenden Elementen:

Devices

Hier wird der Name und das Subsystem des primären Geräts sowie – soweit verfügbar – des sekundären Geräts angezeigt. Durch anwählen des “Wink” Knopfes wird auf dem jeweiligen Gerät ein “Wink” ausgeführt (siehe Abschnitt 6.4.9). Des Weiteren wird das aktuell ausgewählte Gerät angezeigt („selected“) sowie ob eine Kommunikation mit dem Gerät möglich ist („ok“/“fail“). Schließlich wird noch die „Unique Node ID“ bzw. „Neuron ID“ der Diagnoseknoten der Geräte angegeben.

Loop Monitor

Zeigt an, ob die Schleife offen oder geschlossen („ok“) ist bzw. das Bus Loop Monitoring abgeschalten ist.

Twin Monitor

Zeigt den aktuellen Status der Twin Router Überwachung an:

- Twin Router: Zeigt an, ob ein Twin Router installiert ist.
- Status: Zeigt an, ob das Gerät der primäre („primary“), sekundäre („secondary“) Router ist, ob die Initialisierungsphase noch nicht abgeschlossen ist („negotiating“) oder ob der sekundäre Router den ausgefallenen primären Router ersetzt hat.
- CEA-709/CEA-852 Communication: Zeigt an, ob der Router über die CEA-709 bzw CEA-852 Seite erreichbar ist.
- CEA-709/CEA-852 Forwarding: Zeigt an, ob der Router signifikant weniger Pakete von der CEA-709 zur CEA-852 Seite (und umgekehrt) weiterleitet als sein Twin Router. Außerdem wird angezeigt, wenn gar keine Pakete weitergeleitet werden (error).

Node Monitoring Status List

Diese Liste zeigt alle Knoten in der Knotenliste mit ihrem aktuellen Status an. Wenn ein Knoten nicht erreichbar ist oder der Knoten nur von einer Seite erreichbar ist weil der Ring offen ist, so wird dieser Zustand in der Spalte „Node Alarm“ angezeigt. Durch Auswahl von einem oder mehreren Knoten und Auswahl von “Wink selected device(s)” kann auf Knoten eine Wink-Operation durchgeführt werden.

Wenn „automatically refresh data“ angewählt ist, so wird die Anzeige der Daten in einem 15 Sekunden Intervall aktualisiert. Die Anzeige kann über die Schaltfläche „refresh“ auch manuell aktualisiert werden.

10.5.4 Kanalstatistiken

Die Kanalstatistikansicht („Channel Statistics“) zeigt die vom L-IP Redundant gesammelten Kanalstatistikdaten an. Die Seite wird durch Anwahl der „Channel Statistics“ Schaltfläche im L-IP Redundant Plug-In angezeigt (siehe Abbildung 123)

Hinweis: *Die Statistikformationen sind nur im Online Modus, wenn auf das Geräte zugegriffen werden kann, verfügbar.*

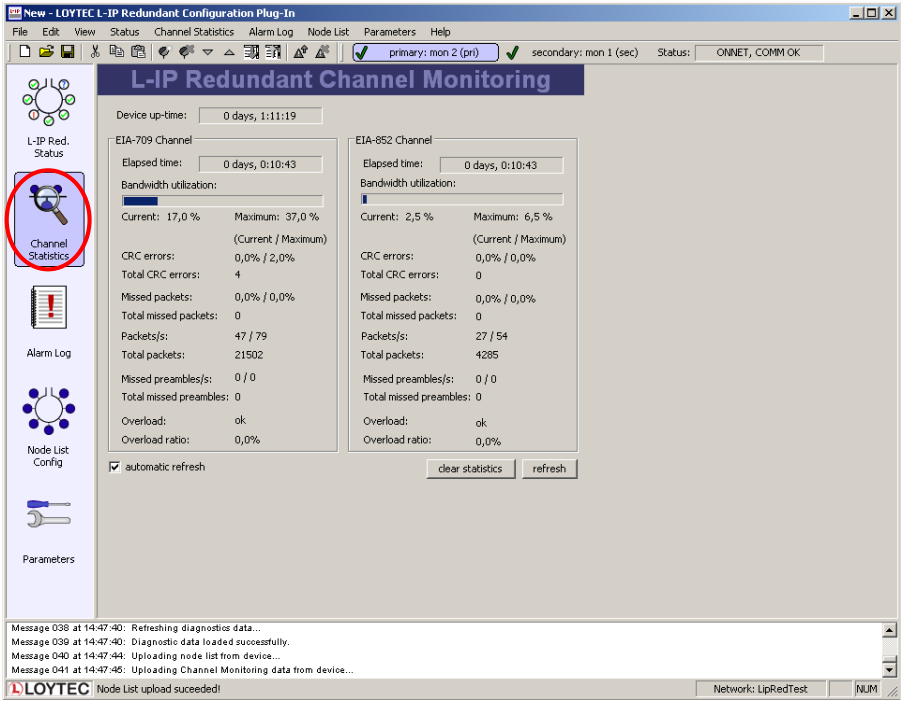


Abbildung 123: Kanalstatistikansicht

Die Gerätestatusansicht besteht aus folgenden Elementen:

Device up-time

Zeigt die Zeit an die vergangen ist seitdem der L-IP Redundant das letzte mal neu gestartet wurde (Kalt- oder Warmstart).

Die folgenden Daten werden für jeden der am L-IP Redundant verfügbaren Kanäle (CEA-709/CEA-852) angezeigt:

Elapsed time

Zeigt die Zeit an die vergangen ist seitdem der L-IP das letzte mal neu gestartet wurde oder seitdem die Statistikdaten für diesen Kanal das letzte mal rückgesetzt wurden.

Bandwidth utilization

Zeigt den aktuellen und den maximalen Wert der Bandbreitenauslastung des entsprechenden Kanals an. Die Balkengrafik zeigt die aktuelle Bandbreitenauslastung.

CRC errors

Zeigt den aktuellen und den maximalen Prozentsatz sowie die absolute Zahl an Paketen mit CRC-Fehler an, die auf dem entsprechenden Kanal empfangen wurden.

Missed Packets

Zeigt den aktuellen und den maximalen Prozentsatz sowie die absolute Zahl an Paketen des entsprechenden Kanals an, die nicht empfangen bzw. verarbeitet werden konnten.

Packets

Zeigt die aktuelle und die maximale Anzahl an Paketen pro Sekunde sowie den die absolute Anzahl an Paketen an, die auf dem entrechenden Kanal beobachtet wurde.

Missed Preambles

Zeigt die aktuelle und die maximale Anzahl an „Missed Preambles“ pro Sekunde sowie den die absolute Anzahl an „Missed Preambles“ an, die auf dem entrechenden Kanal beobachtet wurde. Unter einer „Missed Preamble“ versteht man, wenn der Link Layer eine Preamble empfängt, die kürzer als die definierte Mindestlänge ist. Eine hohe Anzahl von „Missed Preambles“ deutet üblicherweise auf Störungen („Rauschen“) am Kanal hin.

Overload

Zeigt einen Überlastzustand auf dem entsprechenden Kanal im letzten Statistikintervall an. Eine Überlastsituation kann auf Grund einer der folgen Gründe eintreten:

- Die Bandbreitenauslastung im letzten Statistikintervall hat den durch den Parameter „Bandwidth Utilization Limit“ definierten Grenzwert (werkseitige Voreinstellung 70%) überschritten ODER
- Die CRC-Fehlerrate im letzten Statistikintervall hat den durch den Parameter „CRC Error Limit“ definierten Grenzwert (werkseitige Voreinstellung 5%) überschritten ODER
- Der Wert „Missed Packets“ war im letzten Statistikintervall nicht null ODER
- Die Anzahl der „Missed Preambles“ im letzten Statistikintervall hat den durch den Parameter „Missed Preamble Limit“ definierten Grenzwert (werkseitige Voreinstellung ausgeschalten) überschritten.

Overload Ratio

Gibt das Verhältnis von Statistikintervallen in denen sich der entsprechende Kanal im Überlastzustand befunden hat zu der Gesamtzahl der Statistikintervalle an.

Wenn „automatically refresh data“ angewählt ist, so wird die Anzeige der Daten in einem 15 Sekunden Intervall aktualisiert. Die Anzeige kann über die Schaltfläche „refresh“ auch

manuell aktualisiert werden. Mittels des Knopfes „clear statistics“ können alle Statistikdaten rückgesetzt werden.

10.5.5 Alarmlog

Bei Auftreten eines Alarms wird dieser in einer internen Logdatei gespeichert. Diese Logdatei kann maximal 256 Einträge enthalten.

Die Log-Ansicht zeigt die Einträge im Alarmlog an. Diese Ansicht wird über das „Alarm Log“ Symbol auf der linken Seite des L-IP Redundant Plug-In Fensters ausgewählt (siehe Abbildung 124).

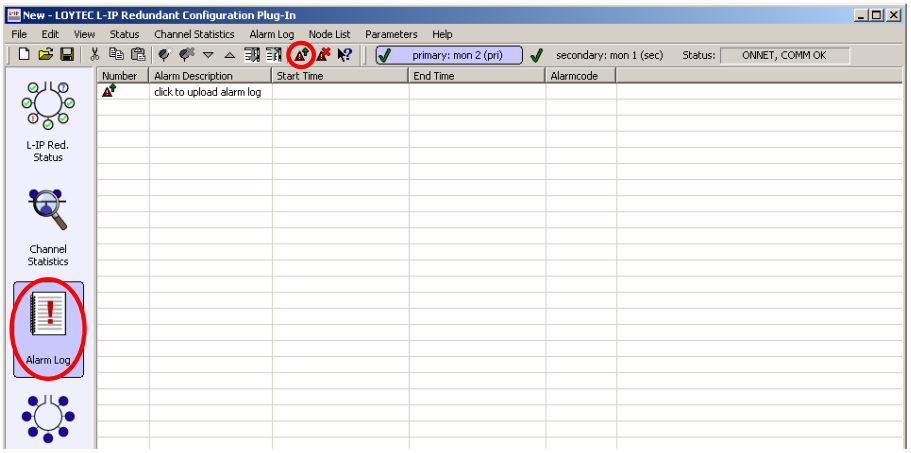


Abbildung 124: Alarmlog-Ansicht

Im Online Modus kann der Alarmlog aus dem Gerät geladen werden. Dazu muss entweder der Eintrag „click to upload alarm log“ mit einem Doppelklick, der Menüeintrag „Upload Alarm Log“ im „Alarm Log“ Menü oder die Entsprechende Schaltfläche in der Werkzeugleiste ausgewählt werden (siehe Abbildung 124). Auf gleiche Weise kann der Alarmlog gelöscht werden.

Abbildung 125 zeigt einen typischen Alarmlog. Für jeden Eintrag wird eine Beschreibung, eine Startzeit, die Endzeit und ein Alarmcode angezeigt. Alle Zeitstempel beziehen sich auf die Uhr im L-IP Redundant. Derzeit sind folgende Alarme definiert:

- "Ring open": Die Schleifenüberwachung hat eine offene Schleife diagnostiziert (siehe Abschnitt 10.2.1).
- "Twin error CEA-709": Twin router kann über die CEA-709 Seite nicht mehr erreicht werden (siehe Abschnitt 10.2.2).
- "Twin error IP": Twin router kann über die CEA-852 Seite nicht mehr erreicht werden (siehe Abschnitt 10.2.2).
- "Fwd warning CEA-709": Anzahl der von der CEA-709 auf die CEA-852 Seite weitergeleitenden Pakete ist deutlich geringer als auf dem Twin Router (siehe Abschnitt 10.2.2).
- "Fwd warning IP": Anzahl der von der CEA-852 auf die CEA-709 s Seite weitergeleitenden Pakete ist deutlich geringer als auf dem Twin Router (siehe Abschnitt 10.2.2).
- "Fwd error CEA-709": Das Geräte leitet keine Pakete von der CEA-709 auf die CEA-852 Seite weiter, der Twin Router jedoch schon.

- "Fwd error IP": Das Geräte leitet keine Pakete von der CEA-852 auf die CEA-709 Seite weiter, der Twin Router jedoch schon.

- "Side 1 disconnect"/"Side 2 disconnect": Twin router kann über Loop Port 1 bzw. Loop Port 2 nicht mehr erreicht werden. Dieser Fehler kann nur auf einem (inaktiven) sekundären Router auftreten.

- "Dev No <no> error" oder "<desc> error": Knoten mit der Nummer <no> oder Beschreibung <desc> ist nicht erreichbar oder nicht "Configured online".

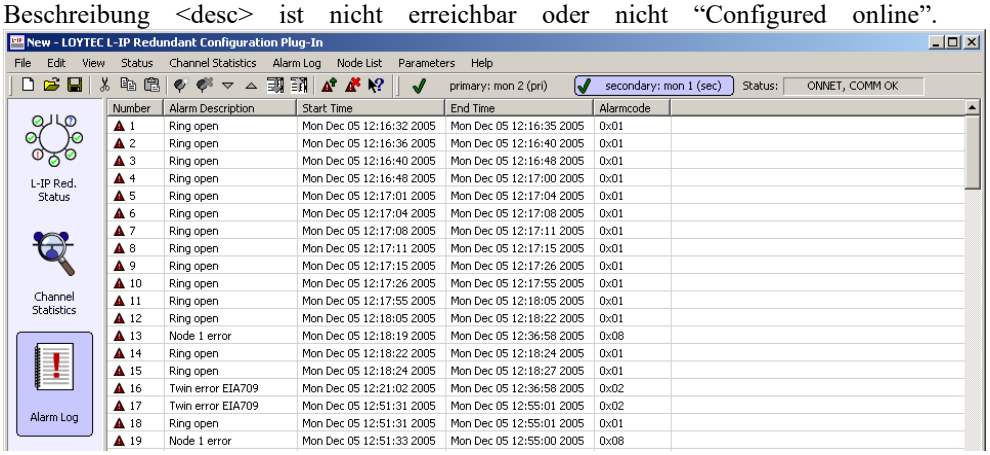


Abbildung 125: Alarmlog

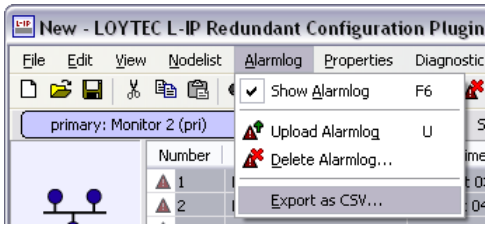


Abbildung 126: Export des Alarmlogs in eine CSV-Datei

Der Alarmlog kann in eine andere Applikation kopiert oder in eine CSV-Datei exportiert werden (siehe Abbildung 126).

10.5.6 Knotenliste

Die Knotenliste wird zur Knotenüberwachung verwendet (siehe Abschnitt 10.2.3). Sie enthält alle Knoten, die von L-IP Redundant überwacht werden. Bei aktiviertem Bus Loop Monitoring sollte die Reihenfolge der Knoten in der Liste mit der Knotenreihenfolge am Kanal übereinstimmen, um bei einem Kabelbruch die Problemstelle lokalisieren zu können. Der Knoten 1 muss dabei dem Anschluss 1 am nächsten liegen, während der letzte Knoten in der Liste am nächsten zu Anschluss 2 ist.

Zur Erstellung oder Änderung einer Knotenliste wechseln Sie zur Knotenlistenansicht, indem sie auf der linken Seite die Schaltfläche "Node List Config" betätigen (siehe Abbildung 127).

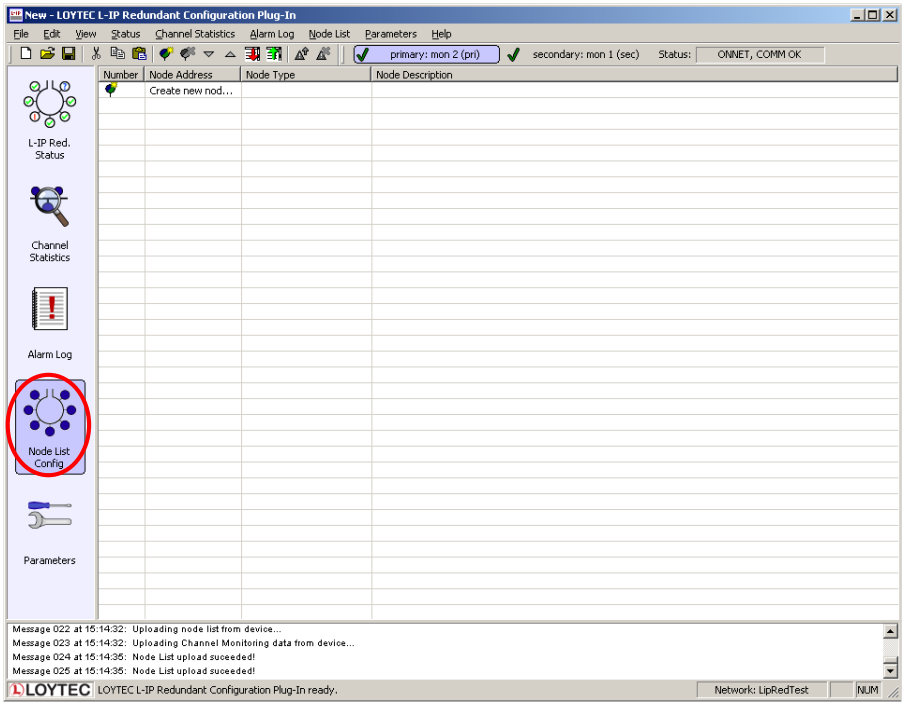


Abbildung 127: Knotenlistenansicht

To create a new node list or edit an existing node list, go to the node list view by clicking on the “Node List Config” icon on the left side of the L-IP Redundant Plug-In window (see Abbildung 127).

Die Knotenliste kann bis zu 128 Knoten enthalten. Knotenlisten können auf drei Arten erstellt werden:

- Import aus einer LNS Datenbank
- Manuelles Eingeben der Knoten
- Import aus einer CSV Datei

Außerdem kann die Reihenfolge der Knoten verändert und die gesamte Liste exportiert werden. Die Liste kann in das Gerät und aus dem Geräte geladen werden.

10.5.6.1 Hinzufügen und Editieren von Knoten

Ein Doppelklick auf “Create new node…”öffnet die „Create new node“ Dialogbox (siehe Abbildung 128).

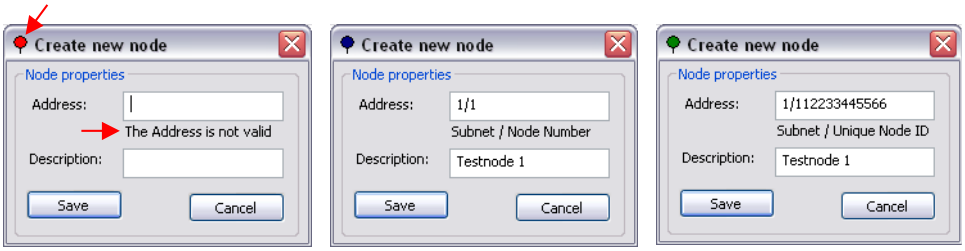


Abbildung 128: Hinzufügen von Knoten

Während der Eingabe wird die Knotenadresse überprüft. Das Ergebnis der Überprüfung wird in der Dialogtitelzeile und in einem Textfeld angezeigt. Mit der “Save” Schaltfläche wird der Knoten in die Knotenliste aufgenommen.

Existierende Knoten können mit einem Doppelklick auf den Listeneintrag editiert werden.

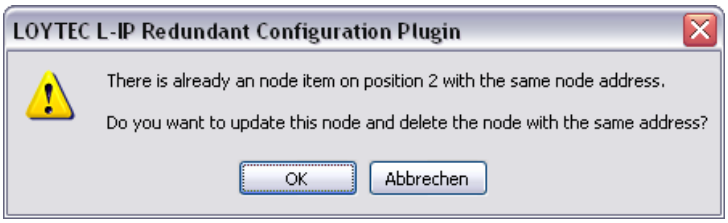


Abbildung 129: Versuch, einen Eintrag mit gleicher Knotenadresse zu speichern

Die Knotenadresse wird auf doppelte Einträge überprüft und gegebenenfalls durch eine Fehlermeldung (siehe Abbildung 130) angezeigt.

10.5.6.2 Importieren der Knotenliste aus einer LNS Datenbank

Die Eingabe von ‘A’ auf der Tastatur oder der entsprechende Eintrag im “Node List” Menü öffnet den Dialog zum automatischen Importieren von Knoten (siehe Abbildung 130).

Sind in der Knotenliste bereits Knoten enthalten so können diese gelöscht oder die neuen Knoten zur bestehenden Liste hinzugefügt werden. Außerdem kann die Adressierungsart gewählt werden, über die der Knoten kontaktiert wird. Zur Wahl stehen Subnet/Node Adressierung oder Neuron-ID Adressierung.

Der LNS-Import steht im Standalone-Betrieb nicht zur Verfügung.

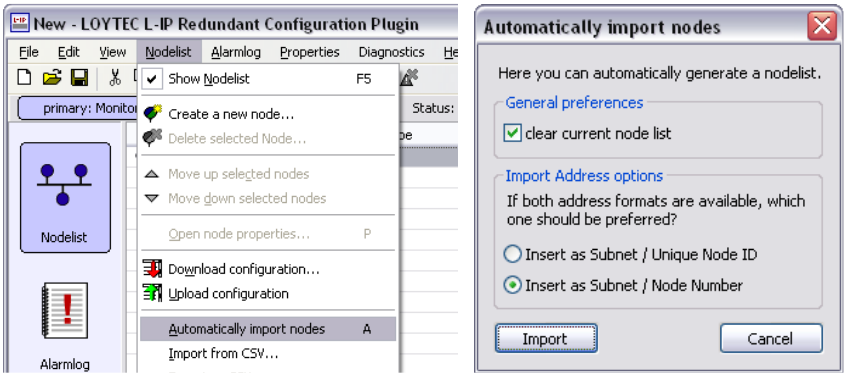


Abbildung 130: Imporrtieren der Knotenliste aus der LNS Datenbank

10.5.6.3 Ändern der Knotenreihenfolge

Um die Reihenfolge der Knoten in der Kontenliste zu verändern, können die Knoteneinträge mit Hilfe der Pfeile in der Werkzeugleiste verschoben werden (siehe Abbildung 131). Mehrere Einträge können durch Drücken der STRG-Taste ausgewählt werden.

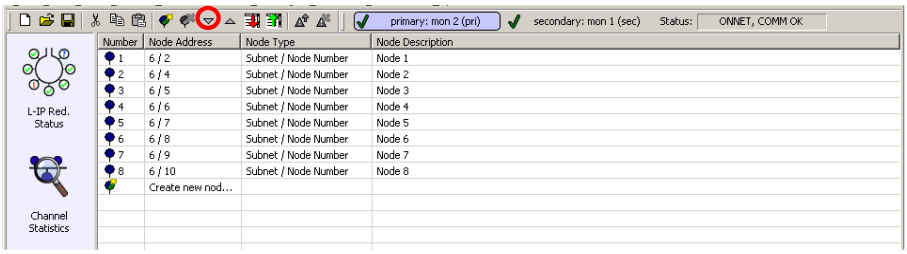


Abbildung 131: Verschieben von Knoten in der Knotenliste

10.5.6.4 Importieren/Exportieren der Knotenliste

Einträge in der Kontenliste können über Kopieren/Einfügen aus anderen Programmen (z.B. Microsoft Excel) übertragen werden. Die übertragenen Felder sind Subnet Adresse, Knotenadresse oder Node ID Adresse und die Beschreibung (siehe Abbildung 132).

Die Knotenliste kann auch aus einer CSV-Datei importiert werden. Dadurch können Programme wie Microsoft Excel zur Erzeugen und zum Editieren der Knotenliste verwendet werden (siehe Abbildung 133).

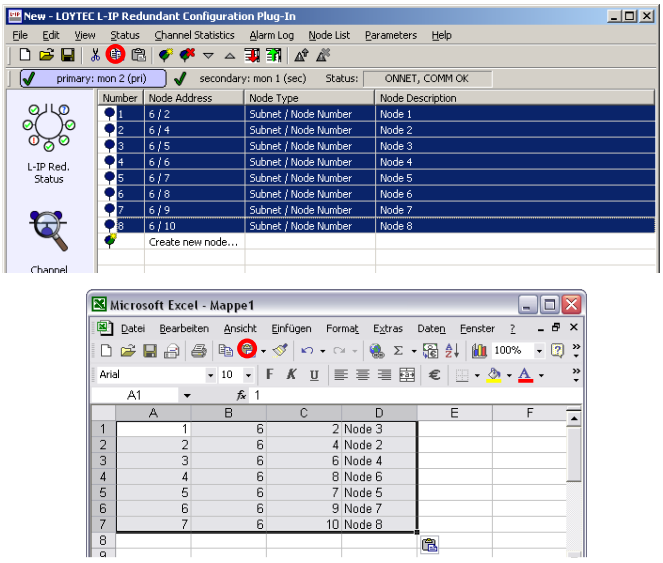


Abbildung 132: Übertragen der Knotenliste über Kopieren/Einfügen

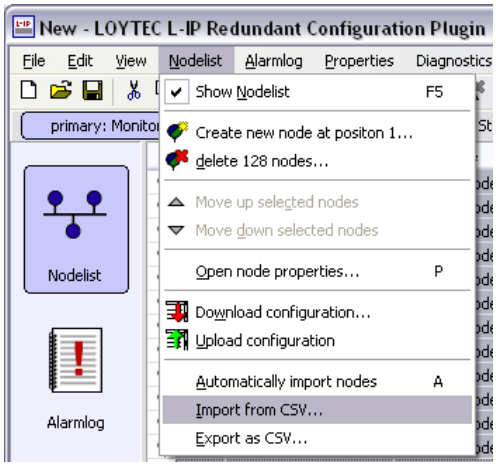


Abbildung 133: Importieren einer CSV Datei

10.5.6.5 Laden und Speichern der Knotenliste

Im Online Modus kann die Knotenliste aus dem L-IP Redundant geladen oder in das Gerät transferiert werden (siehe Abbildung 134).

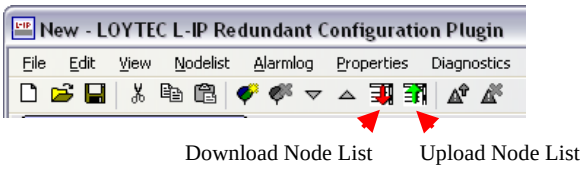


Abbildung 134: Laden und Speichern der Knotenliste

Wenn zwei redundante Router im Twin Router Modus eingesetzt werden so erscheint ein Dialog der fragt, ob die Knotenliste auch in den zweiten Routern („Twin Router“) gespeichert werden soll. Es wird empfohlen, diesen Dialog mit „Yes“ zu bestätigen (siehe Abbildung 135).

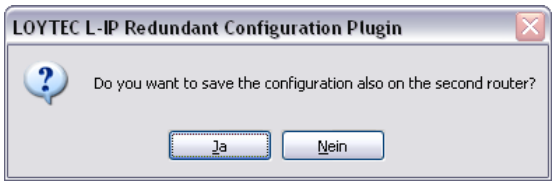


Abbildung 135: der Knotenliste in den Twin Router?

10.5.7 Parameter

Die Parameteransicht wird verwendet, um das Verhalten des L-IP Redundant zu konfigurieren. Die Parameteransicht wird über das Symbol „Parameters“ im L-IP Redundant Plug-In Fenster ausgewählt (siehe Abbildung 136).

Die einzustellenden Parameter sind:

Max Status Send Time

Dieser Wert legt die Heartbeat-Rate im Node Objekt des Diagnoseknotens fest (siehe Abschnitt 10.7.1). Der Wert 0 deaktiviert die Heartbeat-Funktion, jeder andere Wert legt das Intervall fest, indem die Variablen *nvoStatus*, *nvoAlarm* and *nvoAlarm_2* ausgesendet werden.

Enable Loop Monitor

Diese Auswahlfläche aktiviert bzw. deaktiviert die Schleifenüberwachung (siehe Abschnitt 10.2.1).

Max Send Time

Dieser Wert legt die Heartbeat-Rate im Bus Loop Monitor Objekt des Diagnoseknotens fest. Der Wert 0 deaktiviert die Heartbeat-Funktion, jeder andere Wert legt das Intervall fest, indem die Variablen *nvoLoopOK* und *nvoLoopStatus* ausgesendet werden.

Enable Twin Router

Diese Auswahlfläche aktiviert bzw. deaktiviert die Twin Router Überwachung (siehe Abschnitt 10.2.2). Hinweis: Es ist nicht erforderlich, die Twin Router Überwachung auszuschalten wenn kein Twin Router vorhanden ist.

Max Send Time

Dieser Wert legt die Heartbeat-Rate im Twin Router Objekt des Diagnoseknotens fest. Der Wert 0 deaktiviert die Heartbeat-Funktion, jeder andere Wert legt das Intervall fest, indem die Variable *nvoTwinStatus* ausgesendet wird.

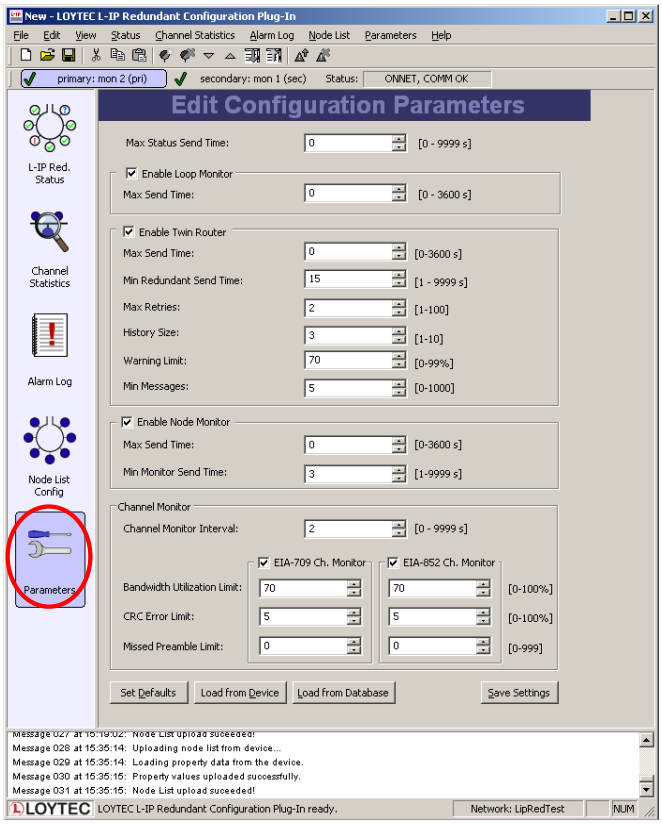


Abbildung 136: : Die Parameteransicht

Min Redundant Send Time

Dieser Wert legt das Intervall zur Twin Router Überwachung fest. Es muss auf beiden Routern identisch sein.

Max Retries

Dieser Wert legt die Anzahl der Wiederholversuche fest, wenn ein Twin Router nicht antwortet. Daher berechnet sich die maximale Zeit, bis ein Ausfall des Twin Routers erkannt wurde, zu:

$$TwinRouter\,FailureDetectionTime \leq Min\,\mathrm{Re}\,dundantSendTime \times (Max\,\mathrm{Re}\,tries + 1)$$

History Size

Dieser Wert legt die Anzahl der Überwachungsintervalle fest die verwendet wird, um die Anzahl der weitergeleiteten Pakete auf beiden Routern zu vergleichen. Dieser Wert muss auf beiden Routern gleich eingestellt werden.

Warning Limit

Dieser Wert legt die Grenze für das "Forwarding Warnings" (siehe *nvoTwinStatus*, Abschnitt 10.7.4 oder Alarmlog, Abschnitt 10.6.3) fest: Ist die Anzahl der weitergeleiteten Pakete des

lokalen Routers kleiner als <*Warning Limit*> % der vom Twin Router weitergeleiteten Pakete, so wird eine Warnmeldung ausgegeben.

Min Messages

Dieser Wert legt die minimale Anzahl von Pakete fest, die weitergeleitet werden muss, um einen "Forwarding Error" (siehe *nvoTwinStatus*, Abschnitt 10.7.4 oder Alarmlog, Abschnitt 10.6.3) auszulösen: Wenn der lokale Router keine Pakete weiterleitet, die Anzahl der vom entfernten Router jedoch zumindest <*Min Messages*> Nachrichten beträgt, so wird ein Alarm ausgelöst. Ist das fehlerhafte Gerät der primäre Router, so übernimmt der sekundäre Router die Kontrolle.

Enable Node Monitor

Diese Auswahlfläche aktiviert bzw. deaktiviert die Knotenüberwachung (siehe Abschnitt 10.2.3).

Max Send Time

Dieser Wert legt die Heartbeat-Rate im Device Monitor Objekt des Diagnoseknotens fest. Der Wert 0 deaktiviert die Heartbeat-Funktion, jeder andere Wert legt das Intervall fest, indem die Variablen *nvoNodeMonAlarm, nvoNodeMonStatus, nvoRingALastNode, nvoRingBLastNode, nvoRingAReceived* und *nvoRingAReceived* ausgesendet werden.

Min Monitor Send Time

Dieser Wert legt das Intervall fest, in dem Query Status Diagnosenachrichten an die Knoten in der Knotenliste gesendet werden. Die maximale Dauer, bis ein Knotenausfall erkannt wird, berechnet sich daher zu:

$$MaxDetectionDelay \leq TotalScanTime = MinMonitorSendTime \times NodesInNodeList$$

Channel Monitor Interval

Dieser Wert legt das Intervall fest, über das die Channel Monitor Objekte ihre Statistikdaten akkumulieren und das benutzt wird um die aktuellen Durchschnittswerte zu berechnen.

CEA-709 Ch. Monitor/CEA-852 Ch. Monitor

Diese Auswahlflächen aktivieren bzw. deaktivieren die entsprechenden Kanalstatistiken (siehe Abschnitt 10.2.3).

Bandwidth Utilization Limit

Dieser Parameter definiert den oberen Grenzwert für die Kanalauslastung. Wird dieser Wert überschritten wird auf dem entsprechenden Kanal eine Überlastsituation angezeigt. Um die Kanalauslastung von der Bestimmung der Überlastsituation auszuschließen muss dieser Wert auf 0 gesetzt werden.

CRC Error Limit

Dieser Parameter definiert den oberen Grenzwert für die CRC-Fehlerrate. Wird dieser Wert überschritten wird auf dem entsprechenden Kanal eine Überlastsituation angezeigt. Um die CRC-Fehlerrate von der Bestimmung der Überlastsituation auszuschließen muss dieser Wert auf 0 gesetzt werden.

Missed Preamble Limit

Dieser Parameter definiert den oberen Grenzwert für die „Missed Preamble" Rate. Wird dieser Wert überschritten wird auf dem entsprechenden Kanal eine Überlastsituation

angezeigt. Um die „Missed Preamble“ Rate von der Bestimmung der Überlastsituation auszuschließen muss dieser Wert auf 0 gesetzt werden.

Im Online Modus werden die Änderungen durch Auswahl der Schaltfläche „Save Settings“ in der LNS Datenbank gespeichert und in das Geräte geladen. Im Offline Modus werden die Werte in der LNS Datenbank gespeichert und beim nächsten Wechsel in den Online Modus in das Gerät übertragen.

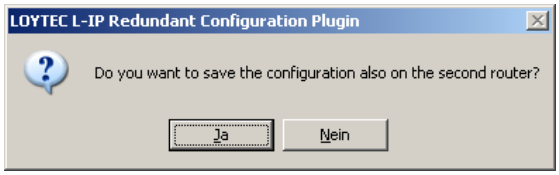


Abbildung 137: Download configuration to second router?

Bei redundantem Routeraufbau können die Daten auch mit dem zweiten Router synchronisiert werden (siehe Abbildung 137). Es wird dringend empfohlen, die Daten in den beiden Routern immer konsistent zu halten.

Um die Parameter auf die Standardwerte rückzusetzten klicken Sie auf den Knopf „Set Defaults“, um die aktuellen Werte aus dem Gerät auszulesen und in der LNS Datenbank zu speichern verwenden Sie den Knopf „Load from Device“.

10.6 Web Interface

Zusätzlich zu den L-IP Einstellungen enthält das Web Interface des L-IP Redundant noch einen Menüeintrag „Redundant“ (siehe Abbildung 138). Darin sind folgende Menüpunkte enthalten:

10.6.1 Status

Abbildung 138 zeigt die Statusseite. Darin enthalten sind die Werte, die auch über die Statusansicht des L-IP Redundant Plug-Ins erreichbar sind (siehe Abschnitt 10.5.3).

Die Unterschiede zum der entsprechenden Ansicht im LNS Plug-In sind:

- Die Anwahl von „Send Service Pin Message“ sendet eine Servicepin-Nachricht des L-IP Redundant Diagnostic Knoten aus.

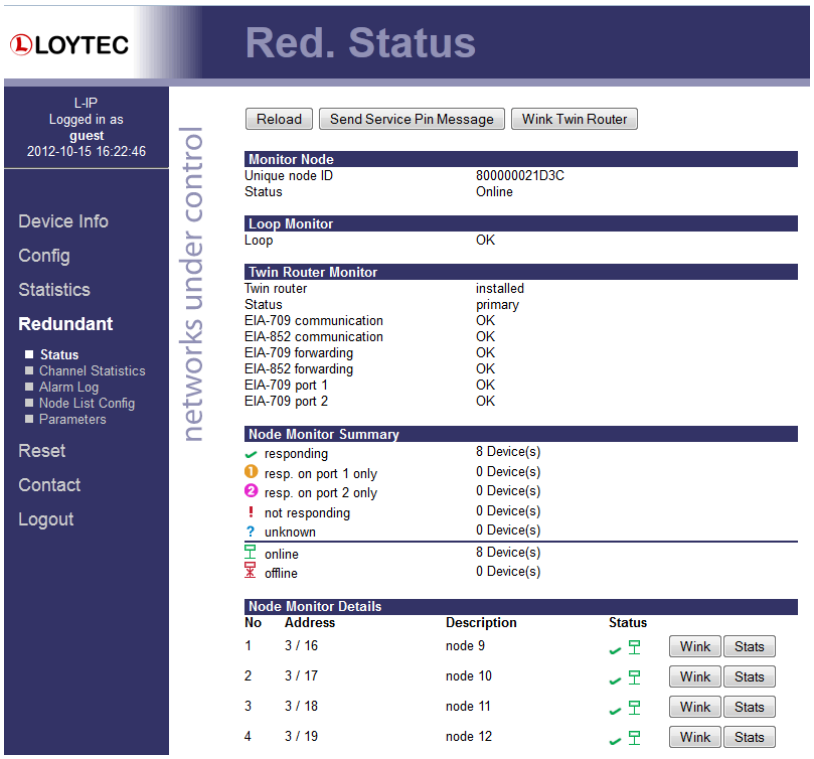


Abbildung 138: The L-IP Redundant Web Interface – Status Page.

- Für jeden erreichbaren Knoten in der Tabelle „Node Monitor Details“ wird eine Schaltfläche „Stats“ angezeigt. Diese Schaltfläche erlaubt die Anzeige der Statistikdaten des entsprechenden Knotens (siehe Abbildung 139).

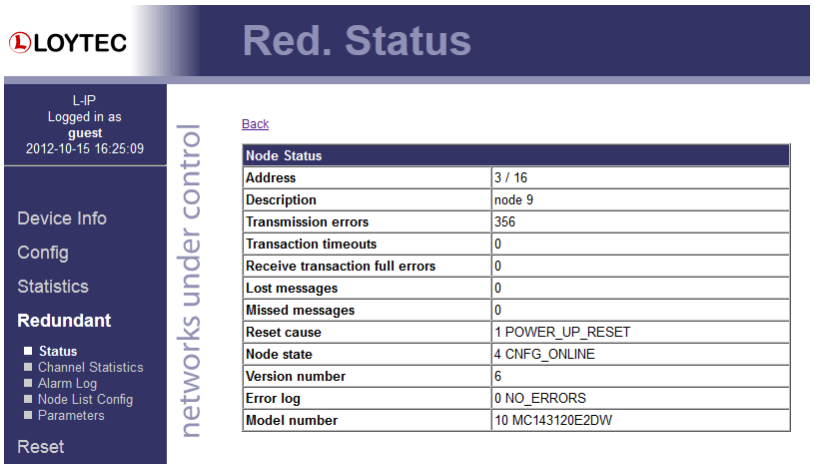


Abbildung 139: Das L-IP Redundant Web Interface – Knotenstatistik

10.6.2 Channel Statistics

Abbildung 140 zeigt die Kanalstatistikseite. Darin enthalten sind die Werte, die auch über die Kanalstatistikansicht des L-IP Redundant Plug-Ins erreichbar sind (siehe Abschnitt 10.5.4).

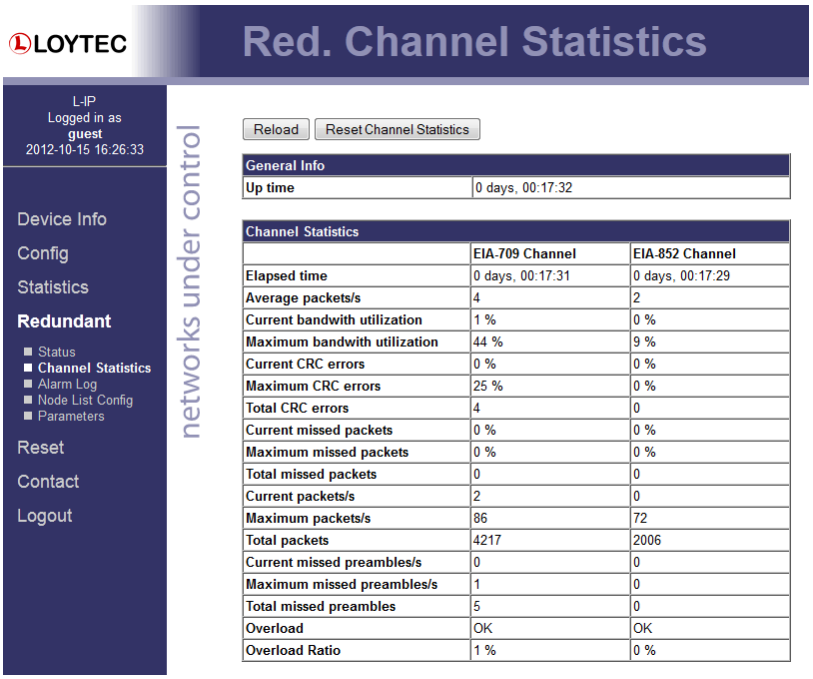


Abbildung 140: Das L-IP Redundant Web Interface – Kanalstatistiken

10.6.3 Alarm Log

Abbildung 141 zeigt die Alarmlog Seite. Die angezeigten Informationen entsprechen denen im L-IP Redundant Plug-In (siehe Abschnitt 10.5.5).

Die Unterschiede zum der entsprechenden Ansicht im LNS Plug-In sind:

Der “Download” Knopf erlaubt, die Logdaten in eine CSV Datei zu speichern.

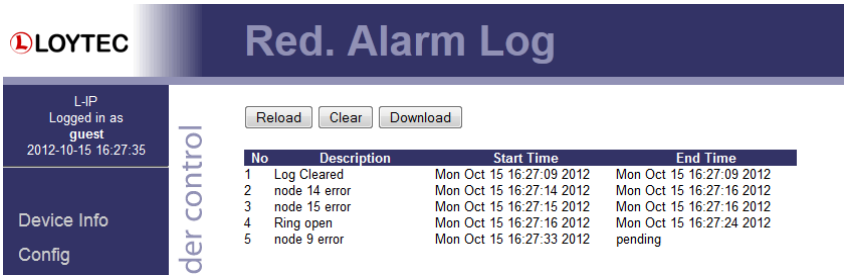


Abbildung 141: Das L-IP Redundant Web Interface – Alarmlog-Seite

10.6.4 Node List Configuration

Abbildung 142 zeigt die Knotenlistenkonfiguration an. Die angezeigten Informationen entsprechen denen im L-IP Redundant Plug-In (siehe Abschnitt 10.5.6) mit folgenden Änderungen:

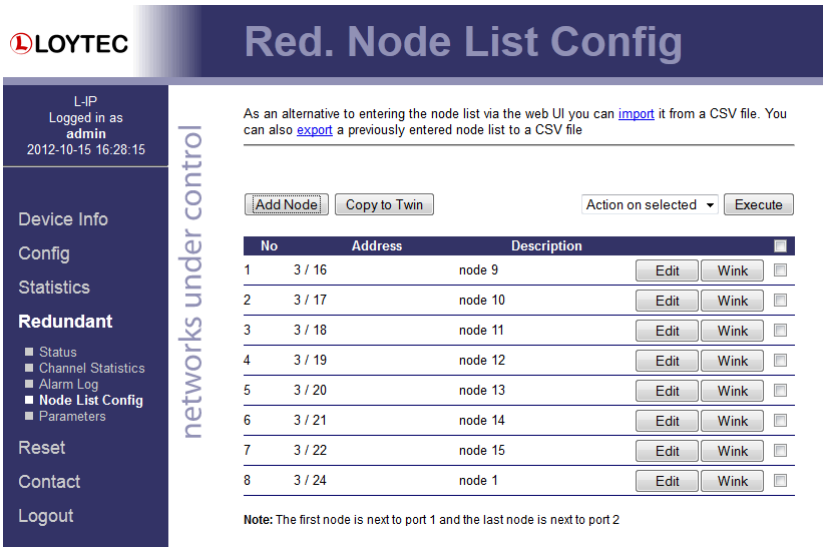


Abbildung 142: Das L-IP Redundant Web Interface – Knotenlistenkonfigurationsseite

- Daten können aus einer CSV Datei importiert (Schaltfläche „import“) und in eine CSV Datei exportiert werden (Schaltfläche „export“).

- Mehrere Knoten können markiert und über eine Auswahlbox („Action on Selected“) verschiedene Aktionen (Move up, Move down, Delete) ausgeführt werden. Der „Execute“ Knopf führt die gewählte Funktion aus.

- Bei Einsatz von redundanten Routern kann mit Hilfe der Schaltfläche „Copy to Twin“ die Konfiguration auf den zweiten Router übertragen werden. Diese Option sollte nach jeder Konfigurationsänderung aufgerufen werden.

10.6.5 Parameter

Abbildung 143 zeigt die Parameterseite an. Die angezeigten Informationen entspreche denen des L-IP Redundant Plug-Ins (siehe Abschnitt 10.5.7) mit folgenden Änderungen:

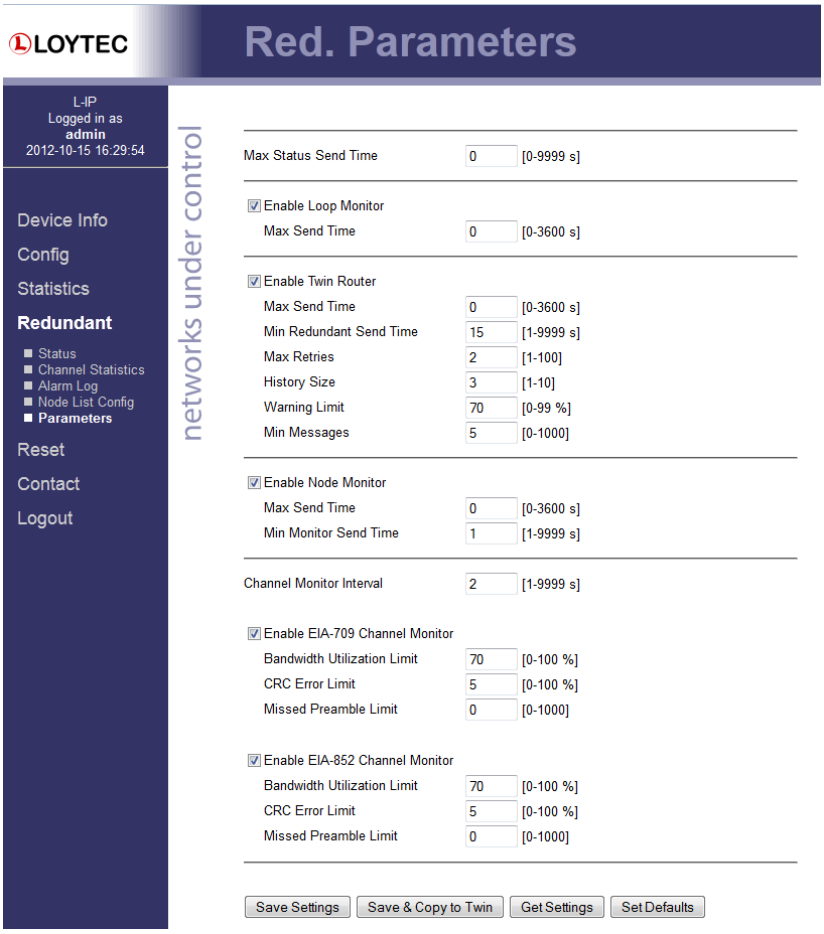


Abbildung 143: Das L-IP Redundant Web Interface – Parameteransicht

Bei redundantem Routereinsatz können die aktuellen Parameter in das Gerät und den Twin-Router geschrieben werden. Es wird empfohlen, die Konfigurationsparameter immer auch in den Twin-Router zu laden.

10.7 Netzwerkschnittstelle

Die Netzwerkschnittstelle wird zur Anzeige, Alarmverarbeitung und Konfiguration zur Verfügung gestellt. Sie folgt den einschlägigen Vorgaben der LONMARK Richtlinien.

10.7.1 Node Object

Der Node Object Funktionsblock ist in Abbildung 144 dargestellt. Zusätzliche zum obligatorischen Interface sind folgende optionale Variablen verfügbar:

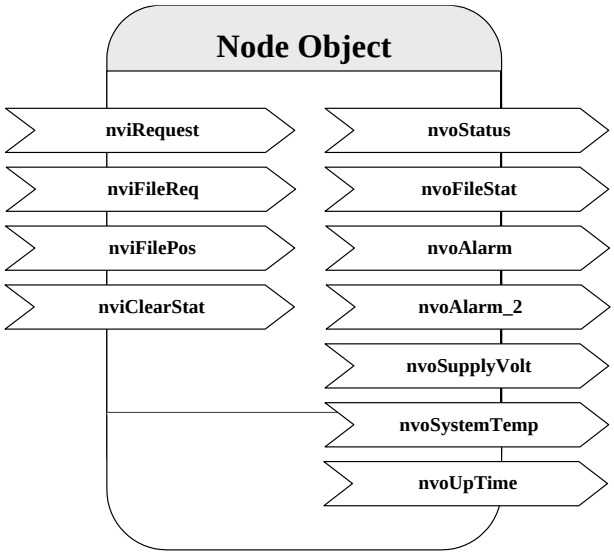


Abbildung 144: Node Object.

- Das Node Object verarbeitet folgende Kommandos über *nviRequest*:
  - RQ_NORMAL
  - RQ_UPDATE_STATUS
  - RQ_REPORT_MASK
  - RQ_ENABLE
  - RQ_DISABLE
  - RQ_UPDATE_ALARM
  - RQ_CLEAR_ALARM
- LonMark alarming wird über nvoAlarm (SNVT_alarm) und nvoAlarm_2 (SNVT_alarm_2) unterstützt. Dadurch können Geräte, die das LonMark Alarm Notifier Profil unterstützen, Alarme von L-IP Redundant Geräten empfangen und entsprechende Aktionen (z. B. Senden einer E-Mail) einleiten. Durch die Unterstützung von beiden Alarm SNVT Typen (SNVT_alarm und SNVT_alarm_2) können sowohl ältere als auch aktuelle Applikationen unterstützt werden.
- Die Netzwerkvariable nvoSupplyVolt (SNVT_volt) zeigt den aktuellen Wert der Versorgungsspannung des L-IP Redundant an, während nvoSystemTemp (SNVT_temp) die aktuelle Gehäusetemperatur bereitstellt. Diese beiden Werte erlauben eine einfache Überprüfung des Hardwarezustandes des L-IP Redundant.
- Die Statistikzähler aller Channel Monitor Objekte (siehe Abschnitt 10.7.5) können rückgesetzt werden indem die Netzwerkvariable nviClearStat (SNVT_switch) auf {100, ON} und zurück zu {0, OFF} gesetzt wird..
- Die Netzwerkvariable nvoUpTime (SNVT_elapsed_tm) enthält die Zeit die vergangen ist seit der L-IP Redundant zuletzt gestartet wurde (Kalt- oder Warmstart).

10.7.2 Bus Loop Monitor Objekt

Abbildung 145 zeigt den Bus Loop Monitor Object Funktionsblock. Dieser Block ist für das Bus Loop Monitoring (siehe Abschnitt 10.2.1) verantwortlich. Es enthält die folgenden Netzwerkvariablen:

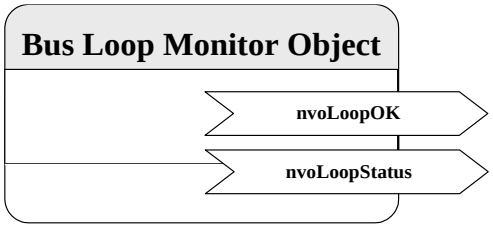


Abbildung 145: Bus Loop Monitor Objekt.

SNVT_switch nvoLoopOK

Diese Variable repräsentiert den aktuellen Status der Ringüberwachung:

- {100, ON}: Der Ring ist geschlossen.
- {0, OFF}: Der Ring ist geöffnet.
- {0, INVAL}: Das Bus Loop Monitoring ist deaktiviert.

SNVT_state_64 nvoLoopStatus

Diese Variable enthält den aktuellen Status des Bus Loop Objekts. Derzeit werden folgende Bits verwendet:

- bit0: 0 wenn Bus Loop Monitoring aktiviert ist, 1 wenn Bus Loop Monitoring deaktiviert ist. Bus Loop Monitoring kann entweder manuell (z.B. deaktivieren des Bus Loop Monitoring Objekts) oder implizit deaktiviert werden, wenn der L-IP im Twin Router Modus ist und das Gerät im Standby-Betrieb arbeitet und daher inaktiv ist.
- bit1: 0 wenn die Schleife geschlossen ist, 1 wenn die Schleife offen ist.

10.7.3 Device Monitor Objekt

Abbildung 146 zeigt den Device Monitor Objekt Funktionsblock. Dieser Funktionsblock ist für die Gerätemonitorfunktion verantwortlich (siehe Abschnitt 10.2.3). Er stellt die folgenden Netzwerkvariablen bereit:

SNVT_state_64 nvoNodeMonStatus

Diese Variable gibt den derzeitigen Status des Device Monitor Objekts an. Zurzeit sind folgende Werte definiert:

- bit0: 0 wenn Device Monitoring aktiviert ist, 1 wenn deaktiviert. Device Monitoring kann entweder manuell (z. B. indem das Objekt deaktiviert wird) deaktiviert werden oder wenn das Gerät im “Twin Router Mode” als sekundärer (standby) Router betrieben wird.
- *bit1*: 0 if all monitored nodes node is reachable and online or was not yet queried, 1 otherwise.

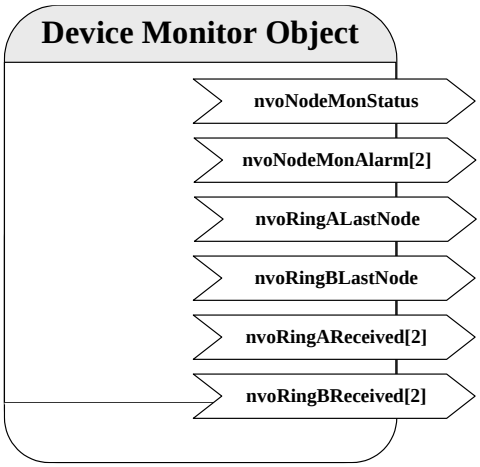


Abbildung 146: Device Monitor Object.

SNVT_state_64 nvoNodeMonAlarm[2]

Zeigt den Status der überwachten Knoten. Jedes Bit entspricht einem Knoten in der Liste, wobei bit0 Knoten 1, Bit 1 Knoten 2, usw. entspricht. Das Element *nvoNodeMonAlarm[0]* entspricht den Knoten 1-64, während *nvoNodeMonAlarm[1]* den Knoten 65-128 zugeordnet ist. Wenn das Bit auf 0 gesetzt ist, so ist der Knoten erreichbar, während ein Wert von 1 einem Fehlerzustand des Knotens (nicht erreichbar oder nicht configured online) darstellt.

SNVT_count nvoRingALastNode

SNVT_count nvoRingBLastNode

Diese beiden Variablen erlauben, den Ort eines Kabelbruchs zu ermitteln. *nvoRingALastNode* enthält den Index des letzten Knotens, der von der Seite 1 erreicht werden kann, während *nvoRingBLastNode* den Wert des letzten erreichbaren Knotens auf Seite 2 entspricht. Die Werte sind wie folgt gespeichert:

- 0: alle Knoten können von dieser Seite erreicht werden (Schleife geschlossen).
- 1-128: Index des letzten erreichbaren Knotens auf dieser Seite
- 0xFFFF: Schleife direkt hinter Router unterbrochen.

Note: *Die Werte sind nur gültig, wenn Bus Loop Monitoring aktiviert ist und die Reihenfolge der Knoten in der Knotenliste der Reihenfolge am Netzwerk entspricht. Ansonsten werden die Werte der Variable auf 0 gesetzt.*

SNVT_state_64 nvoRingAReceived[2]

SNVT_state_64 nvoRingBReceived[2]

Zeigen auf welcher Seite die Knoten zuletzt auf die Query Status Diagnosenachricht geantwortet haben. Jedes Bit entspricht einem Knoten in der Knotenliste, wobei Knoten 1 Bit Index 0 zugeordnet ist. *nvoRingXReceived[0]* repräsentiert die Knoten 1-64, während *nvoRingXReceived[1]* für die Knoten 65-128 verantwortlich ist. Wenn der entsprechende Bitwert in *nvoRingAReceived[X]* auf 1 gesetzt ist, so hat der Knoten auf Seite 1 geantwortet, während ein Bitwert von 1 in *nvoRingBReceived[X]* einer Antwort auf Seite 2 entspricht. Dadurch können die in Tabelle 7 gezeigten Werte zustande kommen:

RingAReceived	RingBReceived	Bedeutung
0	0	Keine Antworten erhalten Knoten antwortet aus einem anderen Subnet über einen Router hinweg Bus Loop Monitoring ist deaktiviert
1	0	Knoten antwortet nur auf Seite 1 Die Schleife ist offen (Kabelbruch)
0	1	Knoten antwortet nur auf Seite 2 Die Schleife ist offen (Kabelbruch)
1	1	Der Knoten antwortet auf beiden Seiten Die Schleife ist geschlossen

Tabelle 7: Bedeutung der *nvoRingXReceived* Bitkombinationen

10.7.4 Twin Router Object

Abbildung 147 zeigt den Twin Router Objekt Funktionsblock. Dieser Funktionsblock ist für den Einsatz der redundanten Router verantwortlich (siehe Abschnitt 10.2.2). Er stellt die folgenden Variablen bereit:

UNVT_red_rtr nviRedRtr

UNVT_red_rtr nvoRedRtr

Wie in Abschnitt 10.4.3.2 erläutert stellen diese beiden Netzwerkvariablen die Verbindung zwischen den beiden L-IP Redundant Geräten her.

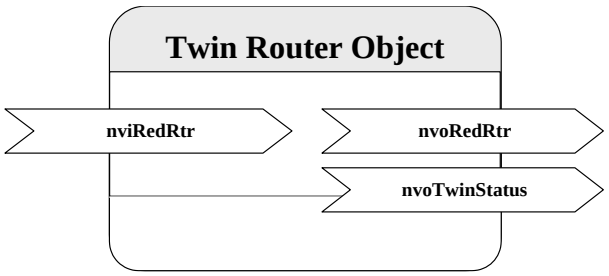


Abbildung 147: Twin Router Objekt.

SNVT_state_64 nvoTwinStatus

Diese Variable gibt den Status des Twin Routers an. Folgende Werte sind derzeit definiert:

- *bit0*: 0 wenn Twin Router Monitoring aktiviert ist. Twin Router Monitoring kann nur manuell deaktiviert werden (z. B. durch Deaktivierung des Objekts).
- *bit1*: 0 wenn das Gerät der sekundäre Router ist, 1 wenn das Gerät der primäre Router ist.
- *bit2*: 0 wenn das Gerät im Normalbetrieb ist (primärer Router aktiv), 1 wenn der Störbetrieb läuft (sekundärer Router aktiv).
- *bit3*: 0 im Normalbetrieb, 1 während der Initialisierungsphase, in der die Rollen des primären und sekundären Routers verteilt werden.
- *Bit4*: 0 wenn die Adresse des anderen Routers noch nicht bekannt ist, 1 wenn sie bekannt ist. Falls die Adresse des anderen Routers noch nicht bekannt ist, so ist der Wert von bit9

(CEA-852 Überwachung) und bit10 bis bit13 (Warnungen und Fehlermeldungen bezüglich des Weiterleitens von Paketen) nicht gültig.

- *bit8*: 1 wenn der andere Router nicht über das CEA-709 Segment erreicht werden kann.
- *bit9*: 1 wenn der Router nicht über den CEA-852 Kanal (IP Backbone) erreicht werden kann.
- *bit10*: 1 wenn die Anzahl der weitergeleiteten Pakete vom CEA-709 Kanal zum CEA-852 Kanal im lokalen Gerät wesentlich geringer ist als die Anzahl des anderen Routers.
- *bit11*: 1 wenn die Anzahl der weitergeleiteten Pakete vom CEA-852 Kanal zum CEA-709 Kanal im lokalen Gerät wesentlich geringer ist als die Anzahl des anderen Routers.
- *bit12*: 1 wenn das lokale Geräte keine Pakete vom CEA-709 Kanal zum CEA-852 weiterleitet, der andere Router jedoch schon.
- *bit13*: 1 wenn das lokale Geräte keine Pakete vom CEA-852 Kanal zum CEA-709 weiterleitet, der andere Router jedoch schon.

10.7.5 Channel Monitor Objekte

Abbildung 148 zeigt den Channel Monitor Objekt Funktionsblock. Dieser Funktionsblock ist für die Netzwerküberwachung verantwortlich (siehe Abschnitt 10.2.3). Für jeden am L-IP Redundant anschließbaren Netzwerkkanal gibt es ein eigenes Objekt. Das Channel Monitor Objekt mit Index 0 ist der CEA-709 Seite des L-IP Redundant zugeordnet, während das Objekt mit Index 1 der CEA-852/IP Seite zugeordnet ist. Jedes dieser Objekte stellt die folgenden Netzwerkvariablen zur Verfügung:

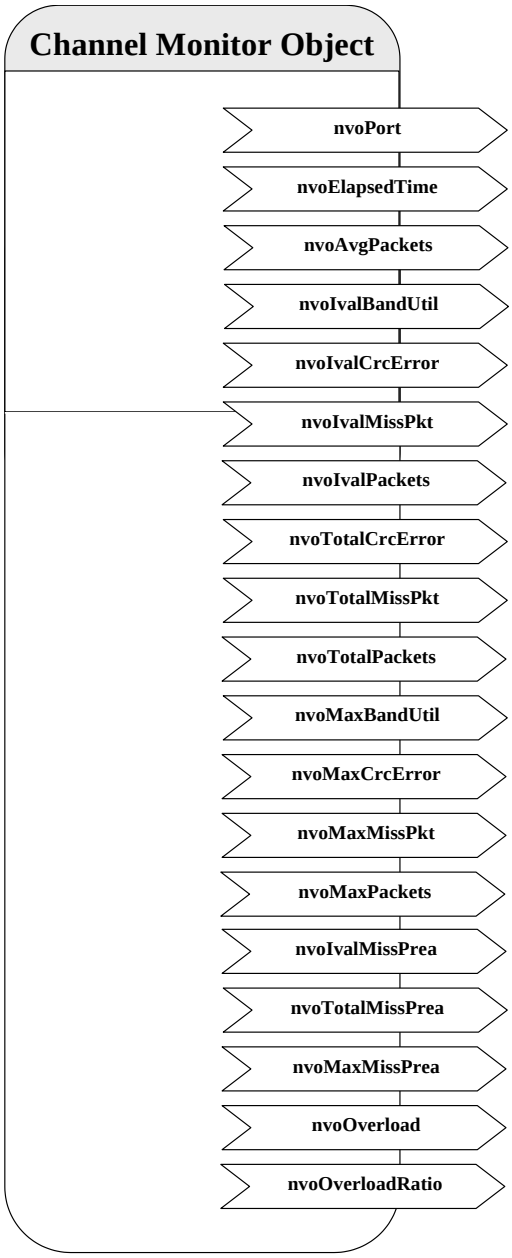


Abbildung 148: Channel Monitor Objekt.

SNVT_count nvoPort

Index des dieser Channel Monitor Objekt Instanz zugeordneten Netzwerkports. Port 1 entspricht der EIA-809 Seite des L-IP Redundant, während Port 2 der CEA-852/IP Seite zugeordnet ist. Nur Polling.

SNVT_elapsed_tm nvoElapsedTime

Zeit die vergangen ist seit die Statistikzähler für dieses Objekt rückgesetzt wurden. Die Statistiken können über Web Interface (siehe Abschnitt 10.6), die Netzwerkvariable *nvoClearStat* (siehe Abschnitt 10.7.1) oder durch einen Reset durch ein Netzwerkmanagementkommando (z.B.: während dem Kommissionieren des Gerätes) rückgesetzt werden. Nur Polling.

SNVT_count_32 nvoAvgPackets

Die durchschnittliche Anzahl an Paketen pro Sekunde auf dem entsprechenden Kanal. Die Bildung des Durchschnitts erfolgt über den Zeitraum seit dem letzten Rücksetzten der Statistikzähler.

SNVT_lev_cont nvoIvalBandUtil

Kanalauslastung des entsprechenden Kanals im letzten Statistikintervall. Für eine zuverlässige Funktion des CEA-709 Netzwerksegments sollte dieser Wert unter 50% liegen.

SNVT_lev_cont nvoIvalCrcError

Prozentsatz an Paketen mit CRC-Fehler am entsprechenden Kanal im letzten Statistikintervall.

SNVT_lev_cont nvoIvalMissPkt

Prozentsatz an Paketen die vom entsprechenden Kanal während des letzten Statistikintervalls nicht empfangen bzw. die nicht verarbeitet werden konnten.

SNVT_count_32 nvoIvalPackets

Anzahl an Paketen pro Sekunde am entsprechenden Kanal während des letzten Statistikintervalls.

SNVT_count_32 nvoTotalCrcError

Gesamtzahl an Paketen mit CRC-Fehler am entsprechenden Kanal seit dem letzten Rücksetzten der Statistikzähler.

SNVT_count_32 nvoTotalMissPkt

Gesamtzahl an Paketen die vom entsprechenden Kanal seit dem letzten Rücksetzten der Statistikzähler nicht empfangen bzw. die nicht verarbeitet werden konnten.

SNVT_count_32 nvoTotalPackets

Gesamtzahl an Paketen pro Sekunde am entsprechenden Kanal seit dem letzten Rücksetzten der Statistikzähler.

SNVT_lev_cont nvoMaxBandUtil

Maximalwert von nvoIvalBandUtil seit dem letzten Rücksetzten der Statistikzähler. Für eine zuverlässige Funktion des CEA-709 Netzwerksegments sollte dieser Wert unter 50% liegen.

SNVT_lev_cont nvoMaxCrcError

Maximalwert von nvoIvalCrcError seit dem letzten Rücksetzten der Statistikzähler.

SNVT_lev_cont nvoMaxMissPkt

Maximalwert von nvoIvalMissPkt seit dem letzten Rücksetzten der Statistikzähler.

SNVT_count_32 nvoMaxPackets

Maximalwert von nvoIvalPackets seit dem letzten Rücksetzten der Statistikzähler.

SNVT_count_32 nvoIvalMissPrea

Anzahl an „Missed Preambles“ pro Sekunde am entsprechenden Kanal während des letzten Statistikintervalls. Unter einer „Missed Preamble“ versteht man, wenn der Link Layer eine

Preamble empfängt, die kürzer als die definierte Mindestlänge ist. Eine hohe Anzahl von „Missed Preambles“ deutet üblicherweise auf Störungen („Rauschen“) am Kanal hin.

SNVT_count_32 nvoTotalMissPrea

Gesamtzahl an „Missed Preambles“ pro Sekunde am entsprechenden Kanal seit dem letzten Rücksetzten der Statistikzähler.

SNVT_count_32 nvoMaxMissPrea

Maximalwert von nvoIvalMissPrea seit dem letzten Rücksetzten der Statistikzähler.

SNVT_switch nvoOverload

Zeigt einen Überlastzustand auf dem entsprechenden Kanal im letzten Statistikintervall an. Eine Überlastsituation kann auf Grund einer der folgen Gründe eintreten:

- Die Bandbreitenauslastung im letzten Statistikintervall hat den durch den Parameter „Bandwidth Utilization Limit“ definierten Grenzwert (werkseitige Voreinstellung 70%) überschritten ODER
- Die CRC-Fehlerrate im letzten Statistikintervall hat den durch den Parameter „CRC Error Limit“ definierten Grenzwert (werkseitige Voreinstellung 5%) überschritten ODER
- Der Wert „Missed Packets“ war im letzten Statistikintervall nicht null ODER
- Die Anzahl der „Missed Preambles“ im letzten Statistikintervall hat den durch den Parameter „Missed Preamble Limit“ definierten Grenzwert (werkseitige Voreinstellung ausgeschalten) überschritten.
- Wird ein Überlastzustand festgestellt so wird die Variable auf {100, ON} gesetzt. Liegt hingegen kein Überlastzustand vor so ist der Wert der Variable {0, OFF}.

SNVT_lev_cont nvoOverloadRatio

Gibt das Verhältnis von Statistikintervallen in denen sich der entsprechende Kanal im Überlastzustand befunden hat zu der Gesamtzahl der Statistikintervalle an.

11 Schnittstellen

11.1 SNMP Interface

Das Simple Network Management Protocol (SNMP) ist ein gängiges Protokoll, um Geräte zu überwachen und zu verwalten. SNMP ist ein Internet-Standard-Protokoll, das von der Internet Engineering Task Force (IETF) definiert wurde. Typischerweise wird es in IT-Umgebungen zum Überwachen von Servern, Routern und Druckern verwendet.

Mit SNMP können Statusinformationen und Statistiken abgefragt werden und über SNMP-Traps Alarme an eine Netzwerkmanagementlösung verschickt werden. Ein verwaltetes Gerät enthält einen SNMP-Agent, der mit dem Netzwerkmanagementsystem mittels UDP kommuniziert. Statusinformationen werden vom SNMP-Agent in einer Baumstruktur verwaltet. Diese wird durch Management Information Bases (MIBs) festgelegt. Eine MIB legt die Namen und Datentypen der verfügbaren Informationen fest. Jedes Datenelement wird dabei von einer Object-ID (OID) identifiziert. Ein Gerät kann eine beliebige Anzahl von MIBs unterstützen, beispielsweise CPU- oder Netzwerkstatistiken.

11.1.1 SNMP Funktionen

LOYTEC-Geräte, welche SNMP unterstützen, weisen folgende Merkmale auf:

- Lese-Zugriff über SNMP Version 2C und 3.
- Standard MIBs: SNMPv2-MIB, SNMPv2-SMI, RFC1213-MIB, IF-MIB, IP-MIB, DISMAN-EVENT-MIB, HOST-RESOURCES-MIB, SNMP-FRAMEWORK-MIB, SNMP-MPD-MIB, SNMP-USER-BASED-SM-MIB, SNMP-VIEW-BASED-ACM-MIB,
- OPC-Datenpunkte können über SNMP ausgelesen werden.
- Eine MIB-Datei für die Datenpunkte eines Geräts kann dynamisch erstellt werden.
- Generische Alarm-Server können SNMP-Traps auslösen.

11.1.2 Konfiguration

Der SNMP-Agent kann über die Webseite des Geräts und über die Konfigurationssoftware konfiguriert werden. Abbildung 149 zeigt die Optionen auf der Webseite. Die Optionen in der Konfigurationssoftware sind analog dazu.

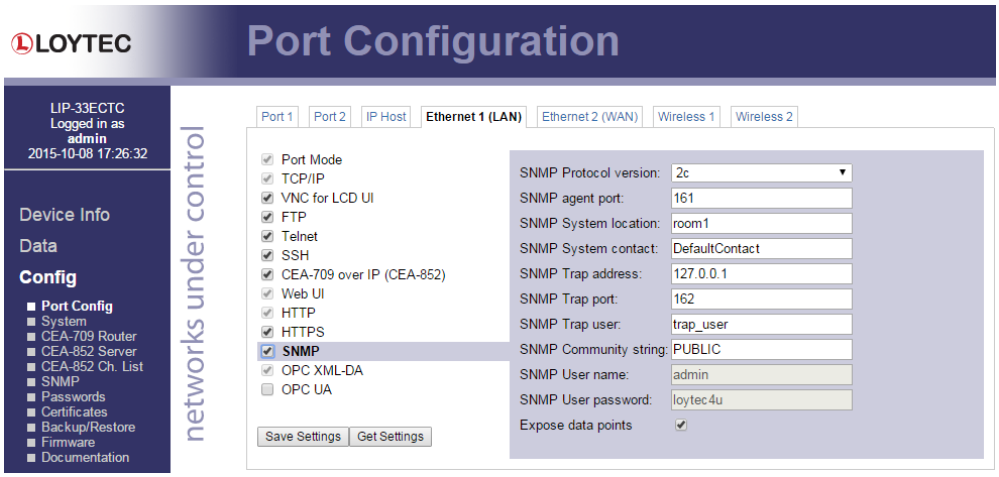


Abbildung 149: SNMP Konfigurationsseite

Die folgenden Einstellungen konfigurieren den SNMP-Agent:

- **SNMP Protocol version**: Diese Einstellung wählt die Protokollversion aus. Mögliche Optionen sind 2C, 3 and 2C+3. Die Protokollversion 2C ist gängiger, bietet aber keine verschlüsselte Authentifizierung.
- **SNMP agent port**: Diese Einstellung wählt den UDP-Port für den SNMP-Agent aus. Es wird empfohlen, die Einstellung auf ihrem Standardwert von 161 zu belassen.
- **SNMP System location:** Diese Einstellung definiert den Wert der `SNMPv2-MIB::sysLocation` OID. Diese OID wird verwendet, um Geräte über SNMP zu lokalisieren.
- **SNMP System contact:** Diese Einstellung definiert den Wert der `SNMPv2-MIB::sysContact` OID. Diese OID wird verwendet, um die für ein Gerät verantwortliche Stelle oder Person zu identifizieren.
- **SNMP Trap address:** Diese IP-Adresse bestimmt den Host, an den SNMP-Traps (Alarme) gesendet werden.
- **SNMP Trap port:** Diese Einstellung definiert den UDP-Port, an den SNMP-Traps (Alarme) gesendet werden.
- **SNMP Trap user:** Diese Einstellung definiert den Usernamen für SNMP-Traps (SNMP v3).
- **SNMP Community string:** Der Community-String ist das Passwort für SNMP v2c.
- **SNMP User name:** Hier wird ein Benutzername für den Zugriff über SNMP v3 festgelegt.
- **SNMP User password:** Hier wird ein Passwort für den Zugriff über SNMP v3 festgelegt.
- **Expose data points:** Mit diesem Schalter können Datenpunkte, die über OPC verfügbar sind, auch über SNMP ausgelesen werden.

11.1.3 Datenpunkte über SNMP

Der SNMP-Agent kann Datenpunkte über SNMP verfügbar machen. Dabei wird jeder Datenpunkt, der über OPC verfügbar ist, auch vom SNMP-Agent angeboten.

Da SNMP Einschränkungen bei den möglichen Datentypen hat, wurden folgende Konventionen getroffen:

- **Binäre Datenpunkte:** Binärdatenpunkte werden auf INTEGER-Datentypen abgebildet. FALSE wird als 0, TRUE als 1 und ein ungültiger Wert als -1 kodiert..
- **Analoge Datenpunkte**: Da es in SNMP keine Gleitkommatypen gibt, werden analoge Datenpunkte durch einen STRING-Datenpunkt abgebildet. Ein ungültiger Wert wird mit "--" kodiert.
- **Multistate-Datenpunkte**: Multistate-Datenpunkte werden auf STRING-Datenpunkte abgebildet. Der Wert entspricht ihrer String-Repräsentation, also beispielsweise AN oder AUS.

SNMP-Variablen müssen innerhalb ihrer MIB eindeutig benannt werden. Daher werden Datenpunkte mit gleichen Namen (in unterschiedlichen Verzeichnissen) durch folgendes Schema eindeutig benannt: `dpNNNNXUUUUUUUU`, beispielsweise `dpFreeMemoryX00000003`. NNNN entspricht dabei dem Datenpunktnamen, wobei alle unzulässigen Zeichen entfernt wurden (erlaubt sind a-z, A-Z und 0-9). UUUUUUUU wird durch die Unique ID (UID) des Datenpunkts ersetzt.

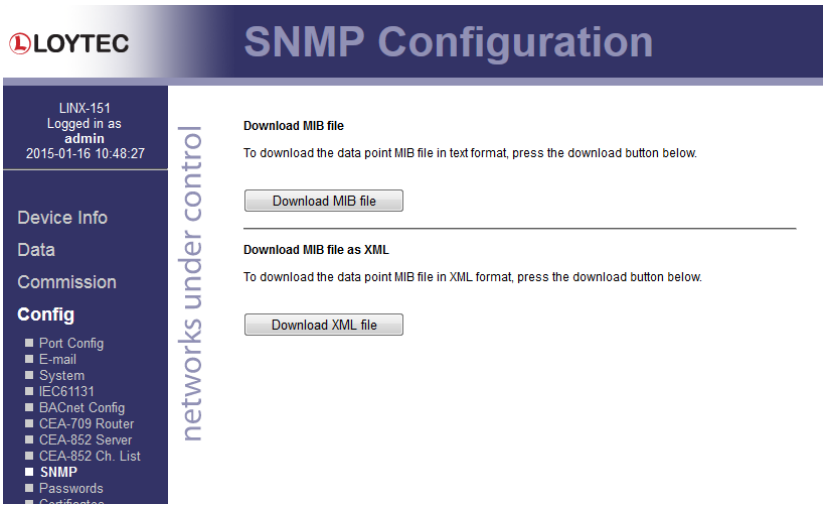


Abbildung 150: Laden von gerätespezifischen MIB-Dateien

Abbildung 150 zeigt die Webseite, von der die gerätespezifische MIB-Datei heruntergeladen werden kann. Mit dem Knopf "Download MIB file" kann eine MIB-Datei heruntergeladen werden, die in ein Netzwerkmanagementsystem importiert werden kann. Mit dem Knopf "Download XML file" erzeugt eine XML-Repräsentation der gerätespezifischen MIB-Datei.

Da die MIB-Datei von der Datenpunktkonfiguration abhängt, führen Änderungen in der Datenpunktkonfiguration zu einer anderen MIB.

11.1.4 SNMP-Sicherheit

Da SNMP sensible interne Informationen anbietet, die für Angriffe auf das Gerät ausgenutzt werden können, sollte SNMP nur in internen und unkritischen Umgebungen eingesetzt werden.

SNMP Version 2C verwendet keinerlei Verschlüsselung. Das Passwort wird im Klartext übertragen und kann einfach aus aufgezeichnetem Netzwerkverkehr extrahiert werden.

SNMP Version 3 überstützt sichere Authentifizierung und Verschlüsselung. LOYTEC-Geräte unterstützen Authentifizierung, aber keine Verschlüsselung der Nutzdaten. Das Passwort wird dabei nicht im Klartext übertragen.

LOYTEC-Geräte unterstützen keine schreibenden Operationen.

12 Netzwerkmedien

12.1 TP-1250

TP-1250-Ports sind mittels Übertragen galvanisch entkoppelt. Ein TP-1250-Kanal muss als Bus verdrahtet werden. Daher müssen beide Enden des Busses mittels eines Netzwerkabschlusses terminiert werden. LOYTEC empfiehlt die Verwendung des L-TERM Netzwerk-Terminators (LT-13) zur terminierung des Netzwerks (siehe Abbildung 151).

Bei deaktiviertem Backbone-Modus (Standardeinstellung) entsprechen die Kommunikationsparameter der TP-1250-Ports eines L-IP der LONMARK-Spezifikation dieses Kanals (TP/XF-1250). Bei eingeschaltetem Backbone-Modus werden proprietäre Kommunikationsparameter verwendet. Daher dürfen in diesem Fall keine Neuron-Chip©-basierenden Knoten oder irgendwelche anderen Knoten mit Standard-TP-1250-Kommunikationsparametern am selben Kanal angeschlossen werden.

12.2 FT-10

Die Kommunikationsparameter der FT-10-Ports eines L-IP entsprechen der LONMARK-Spezifikation für diesen Kanal. Die FT-10-Ports können auch an Link-Power (LP-10) Kanäle angeschlossen werden. Allerdings verfügt der L-IP über keine Spannungsversorgung für den Link-Power Kanal.

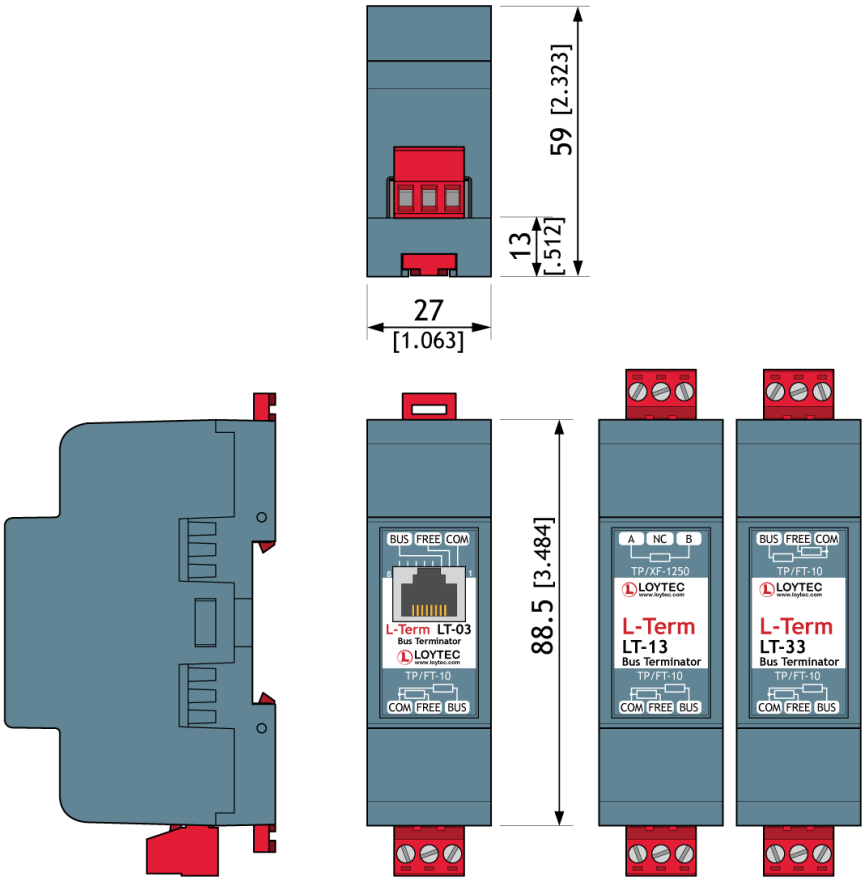


Abbildung 151: FT-10 Netzwerk-Terminator.

Bei Nutzung der freien Topologie wird lediglich ein Netzwerkabschluss an irgendeiner Stelle im Netzwerksegment benötigt. Bei Verwendung der Bustopologie werden zwei Netzwerkabschlüsse an beiden Enden des Busses benötigt.

LOYTEC empfiehlt die Verwendung des L-TERM Netzwerk-Terminators (LT-13, LT-33 or LT-03) zur terminierung des Netzwerks (siehe Abbildung 151).

12.3 RS-485

Die Transceiver-Parameter der RS-485-Ports eines L-IP entsprechen der TIA/EIA RS-485-Spezifikation für diesen Kanal. Maximal 32 RS-485-Ports des L-IP dürfen an einem Netzwerksegment angeschlossen werden.

Der L-IP unterstützt Bitraten zwischen 0,61 kbps und 2,5 Mbps auf seinem RS-485-Port. Bei Verwendung der automatischen Bitratenerkennung werden folgende Bitraten überprüft: 0,61 kbps, 1,221 kbps, 2,441 kbps, 4,883 kbps, 9,766 kbps, 19,531 kbps, 39,0625 kbps, 78,125 kbps, 156,25 kbps, 312,5 kbps, 625 kbps, 1.250 kbps und 2.500 kbps. Für diese Bitraten werden Neuron-Chip©-kompatible Kanalparameter mit 4 Priority Slots verwendet, wobei der Knoten keinen zugewiesen hat. Wird die automatische Bitratenerkennung deaktiviert, so verwendet der L-IP die von LONMARK für den TP-RS485-39-Kanal (39 kbps) spezifizierten Kommunikationsparameter.

RS-485 erfordert ein Netzwerksegment mit Bustopologie, das an beiden Enden mit Netzwerkabschlüssen versehen werden muss. Die maximale Länge einer Stichleitung zwischen der Hauptbusleitung und einem Knoten beträgt 0,3 m.

LOYTEC empfiehlt die Verwendung eines L-TERM Netzwerkterminators (LT-04 oder LT-B4) für den Netzwerkabschluss (siehe Abbildung 152).

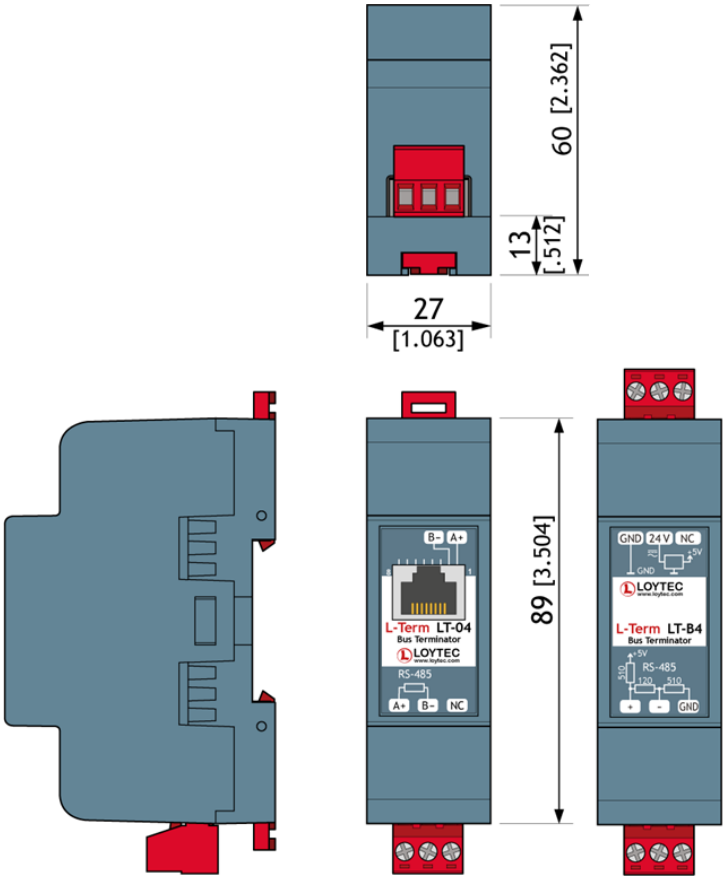


Abbildung 152: Netzwerkabschluss für RS-485.

Der L-IP unterstützt die automatische Erkennung der Bitrate auf RS-485-Kanälen. Die werkseitige Standardeinstellung für den DIP-Schalter ermöglicht die automatische Erkennung der Bitrate an allen RS-485-Ports. Abbildung 153 zeigt die Einstellungen der DIP-Schalter zum Deaktivieren der automatischen Erkennung der Bitrate, vorausgesetzt, alle anderen DIP-Schalter bleiben in der werkseitigen Standardposition.

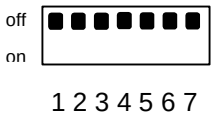


Abbildung 153: DIP-Schalter 3 deaktiviert die automatische Bitratendetektion.

Alternativ kann die automatische Bitratendetektion im Konsolemenü ein- und ausgeschalten werden. Das Konsolemenü erlaubt auch die automatische Bitratendetektion neu zu starten. Während das Port die Bitratendetektion durchführt, blinkt die Activity LED orange.

12.4 Redundante Ethernet-Verkabelung

12.4.1 Verkabelungsoptionen

Die L-IP Modelle der C-Serie verfügen über zwei Ethernet-Ports, die über einen internen Ethernet-Switch verbunden sind. Diese Architektur erlaubt Verkabelungsarten, mit denen die Zuverlässigkeit erhöht und die Verkabelungskosten reduziert werden können. In diesem

Abschnitt bezeichnet der Begriff *upstream* die Richtung zum Netzwerk hin, an dem die Geräte angeschlossen werden. Im Gegenzug bezeichnet der Begriff *downstream* die Richtung vom Netzwerk weg, an dem die Geräte angeschlossen werden.

Die redundante Ethernet-Verkabelung wird durch das Rapid Spanning Tree Protocol (RSTP) ermöglicht, welches von den meisten verwaltbaren (managed) Switches unterstützt wird. Beachten Sie bitte, dass dies ein Feature des Switches und nicht des L-IP ist, weshalb LOYTEC nicht garantieren kann, dass diese Verkabelungsarten mit beliebigen Switches funktionieren. Auf keinen Fall funktioniert eine redundante Verkabelung aber mit nicht verwaltbaren (unmanaged) Switches. Das ältere Spanning Tree Protocol sollte nicht verwendet werden, da es zu lange Konvergenzzeiten aufweist.

Sterntopologie: Im einfachsten Fall ist ein Gerät mit einem Kabel an einem Ethernet-Switch angeschlossen. Dies wird Sterntopologie genannt, da alle Geräte an einem gemeinsamen Upstream-Switch angeschlossen sind. In dieser Topologie stellen das Kabel und der Upstream-Switch eine singuläre Fehlerquelle dar.

Linientopologie: Da der L-IP einen Switch enthält, können diese Geräte miteinander in einer Linie verkettet werden. Dies stellt eine besondere Form der Sterntopologie dar. Der Vorteil liegt in den verringerten Verkabelungskosten. Der Nachteil dieser Topologie liegt in dem Verbindungsabruch zu Downstream-Geräten, wenn ein Upstream-Gerät ausgeschaltet, entfernt oder neu gestartet wird. Außerdem müssen sich alle Geräte der Linie dieselbe Ethernet-Bandbreite (100 MBit/s) teilen. Beim letzten Gerät bleibt ein Ethernet-Port offen, da in Ethernet (ohne STP) keine Schleifen gebildet werden dürfen. Die empfohlene Maximalanzahl an hintereinander geschalteten Geräten ist 20.

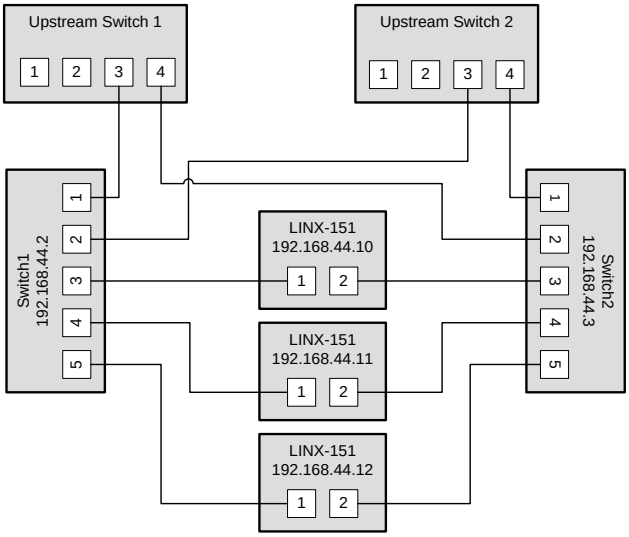


Abbildung 154: Vollredundante Ethernet-Topologie

Vollredundante Ethernet-Topologie: In Abbildung 154 wird eine vollredundante Netzwerkanbindung der L-IP mit den IP-Adressen 192.168.44.10 bis 192.168.44.12 dargestellt. Beide Ethernet-Ports werden an je einen Ethernet-Switch angeschlossen, wobei diese RSTP unterstützen müssen. Es kann dabei der Ausfall eines Kabels oder Switches toleriert werden. Bei dieser Topologie wird die Verfügbarkeit des Geräts erhöht. Als Nachteil entstehen höhere Hardware- und Verkabelungskosten. Die Upstream-Verbindungen erfolgen über die Ports mit der niedrigsten Nummer. Falls dies nicht möglich ist, ist die STP-Priorität für die Upstream-Ports auf den niedrigsten Wert zu stellen (was die höchste Priorität bedeutet).

Ringtopologie: Bei der Ringtopologie werden die Geräte in einer Linie verbunden und die Enden der Linie mit je einem Ethernet-Switch, wobei diese RSTP unterstützen müssen. In Abbildung 155 werden die Geräte mit den IP-Adressen von 192.168.44.10 bis 192.168.44.12

zu einem Ring zusammen geschlossen. Falls ein Gerät ausfällt, entfernt oder neu gestartet wird, berechnen die STP-Bridges einen neuen Spannbaum, sodass nach kurzer Zeit wieder alle Geräte erreichbar sind. Nur falls zwei oder mehr Geräte in der Linie zur selben Zeit ausfallen, sind die dazwischenliegenden Geräte nicht erreichbar. Die empfohlene Maximalanzahl an hintereinander geschalteten Geräten ist 20.

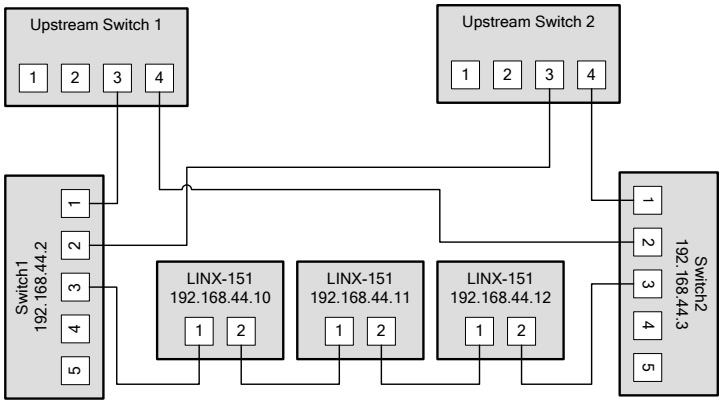


Abbildung 155: Ethernet-Topologie als Ring

12.4.2 Upstream-Varianten

Es gibt mehrere Varianten, wie Switch1 und Switch2 an das Upstream-Netzwerk angebunden werden können.

Einfache Verbindung: Switch1 (oder Switch2, aber nicht beide) wird mit dem Upstream-Netzwerk verbunden. Der andere Switch dient nur dazu, einen redundanten Pfad zu den LOYTEC-Geräten herzustellen. Der redundante Pfad wird durch ein Ethernet-Kabel hergestellt, das direkt Switch1 mit Switch2 verbunden wird. Dieses muss einen niedrigeren Port am Switch verwenden als die L-IP-Geräte. Falls dies nicht möglich ist, muss die STP-Port-Priorität für die Querverbindung auf einen niedrigen Wert gestellt werden. Die RSTP-Domain sollte in dieser Anwendung auf Switch1 und Switch2 beschränkt werden. Dazu wird auf dem Upstream-Switch ein BPDU-Filter aktiviert. Dieser verhindert, dass RSTP-Pakete in das Upstream-Netzwerk gelangen. Ein Beispiel für diese Topologie ist in Abbildung 156 dargestellt.

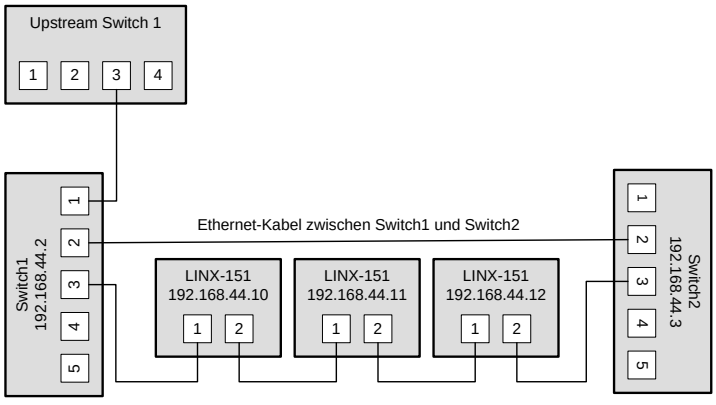


Abbildung 156: Einfache Upstream-Verbindung

Redundante Verbindung; Switch1 und Switch2 sind beide mit dem Upstream-Netzwerk verbunden. Das kann entweder über zwei unterschiedliche Switches im Upstream-Netzwerk erfolgen, oder Switch1 und Switch2 können auf unterschiedlichen Ports am selben Upstream-Switch angeschlossen sein. In dieser Anwendung wird RSTP sowohl für die redundante Anbindung der LOYTEC-Geräte und die redundante Anbindung an das Upstream-Netzwerk

benötigt. Die Konfiguration von Switch1 und Switch2 muss sicherstellen, dass diese beiden Switches nicht zur Root-Bridge gewählt werden. Wenn möglich, sollte die Gerätekommunikation in einem separaten VLAN erfolgen und MSTP (Multiple Spanning Tree Protocol) zum Einsatz kommen. Diese Topologie ist in Abbildung 154 dargestellt.

12.4.3 Voraussetzungen

Für die vollredundante Topologie und die Ringtopologie müssen folgende Voraussetzungen erfüllt sein:

- Die Upstream-Switches müssen das Rapid Spanning Tree Protocol (RSTP) unterstützen, welches durch den Standard IEEE 802.1w definiert wird. Die Upstream-Switches müssen über einen Broadcast-Storm-Filter verfügen.
- Beide Enden des Ringes müssen an unterschiedlichen Switches angeschlossen werden.
- Beide Upstream-Switches müssen mit demselben Ethernet-Netzwerk verbunden sein.

12.4.4 Switch-Konfiguration

Die Switches, über welche die Geräte mit dem Netzwerk verbunden werden, benötigen die folgenden Einstellungen. Diese stellen eine Empfehlung dar, welche je nach Switch-Modell unterschiedlich umgesetzt werden muss. Jedes redundante Netzwerk muss nach der Konfiguration getestet werden, damit die Umschaltung zuverlässig funktioniert und Netzwerkschleifen vermieden werden.

- Die STP-Bridge muss aktiviert sein.
- Die STP-Priorität sollte auf den minimalen Wert (61440) eingestellt werden, damit dieses Switches nicht als Root-Bridge ausgewählt werden.
- Der Bridge-Mode sollte dem Bridge-Mode des restlichen Netzwerkes entsprechen, bevorzugterweise 802.1s or 802.1w.

Falls das Upstream-Netzwerk RSTP verwendet, müssen dessen Timing-Parameter übernommen werden. Ansonsten sollten die Zeitparameter der STP-Bridge auf die minimalen Werte einstellt werden, um die kürzestmögliche Konvergenzzeit zu erzielen:

- Maximales Alter (Bridge max age time): 6 Sekunden
- Hello-Zeit (Hello time): 1 Sekunden
- Weiterleitungsverzögerung (Forward delay): 4 Sekunden
- Alle Switch-Ports, die Schleifen bilden, dürfen **nicht** als EDGE-Ports konfiguriert sein, da ansonsten Paketschleifen entstehen können.
- Die Broadcast-Storm-Filter der Switches sollten aktiviert werden. Mögliche Vorgaben wären 5% or 3000 Pakete/s.

Die Upstream-Switches benötigen die folgende Konfiguration:

- Bei einer einfachen Upstream-Verbindung sollte der verwendete Port des Upstream-Switches BPDU-Filtering aktiviert haben.
- Bei einer redundanten Upstream-Verbindung sollte der verwendete Port des Upstream-Switches BPDU-Root-Guard aktiviert haben.

12.4.5 Verbindungstests

Sobald die Geräte und die Switches konfiguriert und verbunden sind, sollten folgende Tests durchgeführt werden. Diese Tests sollen das Umschaltverhalten der STP-Bridges überprüfen, damit die Topologieänderungen beim Umschalten keine Auswirkungen auf das restliche Netzwerk haben.

- Überprüfen Sie, dass keine Broadcast-Storms im Netzwerk auftreten. Das kann durch Aufzeichnen des Verkehrs zwischen Switch1, Switch2 und dem Upstream-Switch erfolgen. Dieser Test sollte während der gesamten Testzeit erfolgen, insbesondere während der Umschaltvorgänge.
- Überprüfen Sie, dass alle Geräte erreichbar sind (ICMP ping).

Führen Sie diese Tests in folgenden Situationen aus:

- Schalten Sie alle Switches und Geräte ein. Wenn alle Geräte gebootet haben, führen Sie die obigen Tests aus.
- Schalten Sie den Switch1 aus. Warten Sie für etwa 10 Sekunden und führen Sie dann die obigen Tests aus.
- Schalten Sie den Switch2 ein und den Switch1 aus. Warten Sie bis der Switch2 gebootet hat und führen Sie dann die obigen Tests aus.
- Schalten Sie den Switch1 ein. Warten Sie bis der Switch1 gebootet hat und führen Sie dann die obigen Tests aus.
- Starten Sie alle LOYTEC Geräte neu. Warten Sie bis die Geräte gebootet haben und führen Sie dann die obigen Tests aus.
- Entfernen Sie ein einzelnes Ethernet-Kabel. Warten Sie für etwa 10 Sekunden und führen Sie dann die obigen Tests aus. Dieser Test sollte für mehrere Kabel wiederholt werden. Auf jeden Fall sollten folgende Verbindungen getestet werden:
  - Die Verbindung zwischen Switch1 und dem L-IP, der direkt an Switch1 angeschlossen ist.
  - Die Verbindung zwischen Switch2 und dem L-IP, der direkt an Switch2 angeschlossen ist.
  - Eine Verbindung in der Mitte der Kette, die weder an Switch1, noch an Switch2 direkt angeschlossen ist.

12.4.6 Beispielskonfiguration für Switches

Das folgende Beispiel zeigt die Konfiguration (anhand von HP Procurve Switches) von Switch1, Switch2 und den Upstream-Switches für die Topologie in Abbildung 154.

Upstream switches:

```
config
spanning-tree
spanning-tree priority 8
spanning-tree 3,4 root-guard
spanning-tree hello-time 1
spanning-tree forward-delay 4
spanning-tree maximum-age 6
exit
```

Switch1 und Switch2:

```
config
spanning-tree
spanning-tree priority 15
spanning-tree 1,2 port-priority 0
spanning-tree 3-5 port-priority 8
spanning-tree hello-time 1
spanning-tree forward-delay 4
spanning-tree maximum-age 6
exit
```

12.5 WLAN

12.5.1 Einleitung

Geräte mit USB-Anschluss, welche den LWLAN-800 WLAN-Adapter unterstützen, können in IEEE 802.11 Drahtlosnetzwerke eingebunden werden. Die folgenden Betriebsmodi werden dabei unterstützt:

- **Client mode (separate network)**: In diesem Modus verbindet sich das Gerät zu einem bestehenden Access Point. Die Firewall der WLAN-Schnittstelle kann dabei den Zugriff auf einzelne Protokolle beschränken. Beispielsweise kann die Konfigurationswebseite des Geräts über WLAN erreichbar sein, nicht aber die BACnet-Kommunikation.

- **Access point mode (separate network)**: Im Access-Point-Modus erstellt das Gerät ein WLAN-Segment zu dem sich WLAN-Clients verbinden können. Im isolierten Modus weist das Gerät den Clients IP-Adressen zu und leitet alle Netzwerk-Zugriffe auf sich selbst um. In diesem Modus kann das Gerät komfortabel mit mobilen Geräten konfiguriert werden.

- **Access point mode (bridged)**: Im gebridgten Access-Point-Modus ist das WLAN-Interface mit einem Ethernet-Interface verbunden. WLAN-Clients können auf Geräte im Ethernet-Netzwerk zugreifen. In diesem Modus ist der DHCP-Server deaktiviert, um Störungen mit einem existierenden DHCP-Server im Ethernet-Netzwerk zu verhindern.

- **Mesh point (separate network)**: In diesem Modus ist das Geräte ein IEEE 802.11s Mesh-Point. Mesh-Points kommunizieren mit anderen Mesh-Points innerhalb in ihrer Funkreichweite und wählen automatisch den besten Weg zum Zielknoten aus. Mit Mesh-Netzwerken können redundante Funkverbindungen aufgebaut werden und ausgedehnte Funknetzwerke aufgebaut werden.

- **Mesh point (bridged)**: Dieser Modus ist wie der Mesh-Point-Modus, nur ist zusätzlich das WLAN-Interface mit einem Ethernet-Interface verbunden. Daher können andere Mesh-Points über dieses Gerät auf Knoten im Ethernet-Netzwerk zugreifen. In einem Netzwerk darf nur ein Mesh-Portal existieren, um Netzwerkschleifen zu vermeiden.

Der LWLAN-800-Adapter kann zwei WLAN-Funktionen gleichzeitig ausführen, was komplexere Konfigurationen ermöglicht, wie beispielsweise:

- Wireless 1 wird als isolierter Access-Point zur Gerätekonfiguration verwendet, während Wireless 2 für die Teilnahme an einem Mesh-Netzwerk verwendet wird.

- Wireless 1 wird als gebridgter Access-Point zur Gerätekonfiguration und zur Konfiguration anderer Geräte am Ethernet-Segment verwendet, während Wireless 2 im Client-Modus verwendet wird, um ein abgesetztes Gerät zu erreichen..

Die beiden WLAN-Funktionen können allerdings nicht komplett unabhängig konfiguriert werden:

- Beide Funktionen müssen das selbe Funkband verwenden.
- Beide Funktionen müssen den selben Funkkanal verwenden.

12.5.2 802.11s Mesh-Netzwerke

WLAN-Client- und Access-Point-Modi ähneln den üblichen Funktionen, die in WLAN-Netzwerken verwendet werden. Dieser Abschnitt beschreibt die Funktionen und Vorteile des 802.11s-Mesh-Netzwerks.

In einem Mesh-Netzwerk gibt es keine Client- und Access-Point-Rollen. Jeder Knoten eines Mesh-Netzwerks sendet und empfängt seine eigenen Daten, leitet aber auch Daten für andere Knoten weiter. Die Knoten beobachten die Qualität der Funkverbindungen und verteilen diese Informationen im Mesh-Netzwerk. Daher können Knoten, die nicht in gegenseitiger Funkreichweite sind, dennoch miteinander kommunizieren. In diesem Fall wird ein Pfad durch das Mesh-Netzwerk bestimmt und die dazwischen liegenden Knoten übertragen die Daten über mehrere Zwischenstationen.

Nachdem sich die Signalstärke und damit die Reichweite verändern kann, Knoten entfernt und hinzugefügt werden können, können sich die günstigen Pfade durch das Mesh-Netzwerk mit der Zeit verändern. Das 802.11s-Routing-Protokoll reagiert auf diese Änderungen und passt die Pfadauswahl entsprechend an.

Das 802.11s-Protokoll enthält auch das AuthSAE-Protokoll (Simultaneous Authentication of Equals), womit jede Funkverbinden mit einem starken Schlüssel gesichert wird. Dieses Protokoll ist resistent gegen passive, aktive und Wörterbuchattacken, solange ein guter Schlüssel gewählt wird.

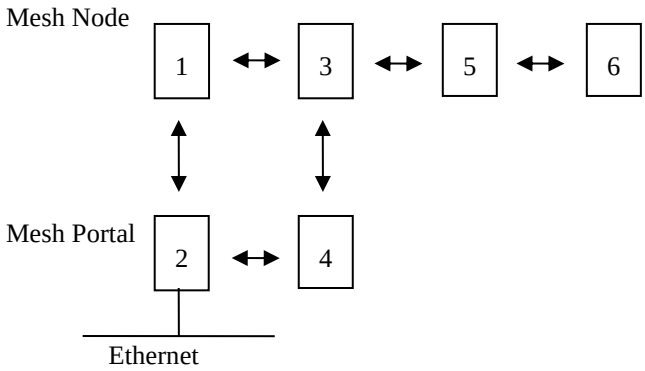


Abbildung 157: Mesh-Netzwerke

Abbildung 157 zeigt die Rollen der Mesh-Points und mögliche Funkverbindungen. Mesh-Point 1 kann direkt mit den Mesh-Points 2 und 3 kommunizieren. Über das Routing-Protokoll erfährt er, dass Ethernet-Netzwerk über Mesh-Point 2 angebunden ist. Damit wird der Netzwerkverkehr, der das Mesh-Netzwerk verlassen soll, automatisch an Mesh-Point 2 weiter geleitet.

Mesh-Point 4 kann direkt mit Mesh-Point 2 und 3 kommunizieren, nicht aber mit Mesh-Point 1. Dadurch haben die Mesh-Points 1 und 4 zwei mögliche Routen und können den Ausfall

von Mesh-Point 2 oder 3 tolerieren. Ein Mesh-Netzwerk ist resistent gegen einzelne Knotenausfälle oder schwankende Qualität der Funkverbindungen.

Am Beispiel von Mesh-Point 6 sieht man, wie ein Mesh-Netzwerk die Reichweite eines Funknetzwerkes erhöhen kann. Wenn Mesh-Point 2 mit Mesh-Point 6 kommuniziert, können zwei mögliche Pfade gewählt werden: 2-4-5-6 and 1-3-5-6. Dabei wird der bessere Pfad ausgewählt und Mesh-Point 5 erhöht die Reichweite des Funknetzwerks.

Dieses Beispiel zeigt, wie zusätzliche Mesh-Points das Netzwerk unempfindlicher gegen Ausfälle macht und die Reichweite des Netzwerks deutlich über der Reichweite einer einzelnen WLAN-Zelle liegt.

12.5.3 Hardware-Installation

Schließen Sie den LWLAN-800-Adapter mit einem USB-Kabel an das Gerät an. Danach schalten Sie die Stromversorgung des Geräts ein. Es wird empfohlen, die USB-Verbindung im Betrieb nicht zu unterbrechen.

Der LWLAN-800 hat zwei Antennenanschlüsse. Die Antennen müssen außerhalb metallischer Gehäuse angebracht werden.

13 L-IP Firmware Update

Die Firmware eines L-IP kann über das CEA-709-Netzwerk, das Ethernet Netzwerk und über die serielle Konsole aktualisiert werden.

Um sicherzustellen, dass der L-IP nicht durch ein fehlgeschlagenes Firmware-Update zerstört werden kann, besteht die L-IP-Firmware aus zwei Teilen:

- dem Fall-Back-Image und
- dem primären L-IP-Firmware-Image.

Das Fall-Back-Image ist in einem schreibgeschützten Bereich des Flash-Speichers abgelegt. Es enthält lediglich jene Teile, die notwendig sind, um ein neues primäres L-IP-Firmware-Image über das Netzwerk in den L-IP zu schreiben. Ferner sorgt es dafür, dass sich der L-IP nach dem Startvorgang in jedem Fall in einem definierten Zustand befindet und somit die Kommunikation über das Netzwerk garantiert ist (z.B. Rücksetzen der Kommunikationsparameter).

Falls der L-IP im Fehlerfall mit dem Fall-Back-Image gestartet wurde, so blinken die CEA-709 Activity LED und die STATUS LED rot. In diesem Zustand werden keine Nachrichten weitergeleitet.

13.1 Firmware-Update über das Web-Interface

Die Firmware des Geräts kann auch über das Web-Interface aktualisiert werden. Diese Option steht unter dem Menü **Config** im Punkt **Firmware** zur Verfügung. Für mehr Informationen dazu lesen Sie bitte den Abschnitt 7.6.2.

13.2 Firmware Update über IP

Um die Firmware über IP auf das Gerät zu laden, muss der L-IP eine gültige IP-Konfiguration haben (siehe Abschnitt 5.2). Weiters benötigen Sie das LOYTEC L-852 Download Tool, welches Sie von unserer Web-Seite www.loytec.com laden können.

Wenn diese Software ausgeführt wird, erscheint ein Fenster wie in Abbildung 158 gezeigt. Geben Sie die **IP Address** des L-IP ein, der aktualisiert werden soll. Wählen Sie die Firmware-Datei '*.dl' im Feld **Firmware File** aus. Optional wählen Sie den Haken **Reboot device after download** und drücken den Knopf **Start Download**.

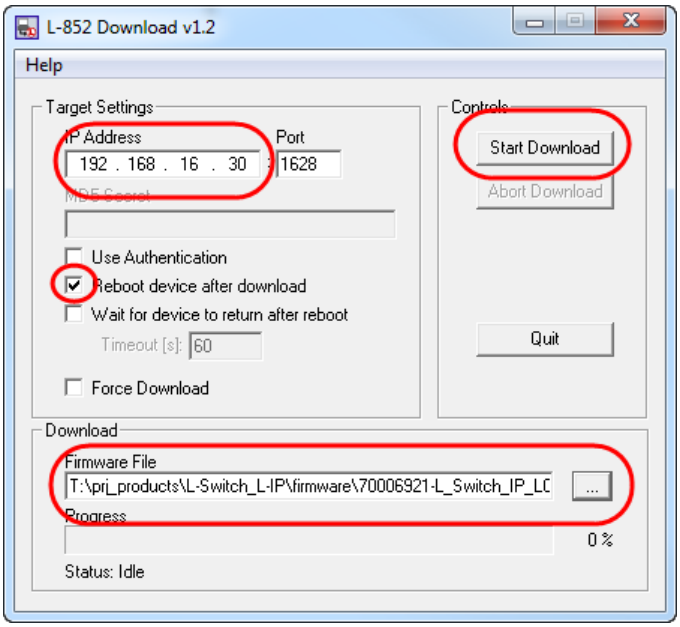


Abbildung 158: Das L-852 Download Tool

Wurde die Aktualisierung erfolgreich abgeschlossen, erscheint das Fenster wie in Abbildung 159 gezeigt.

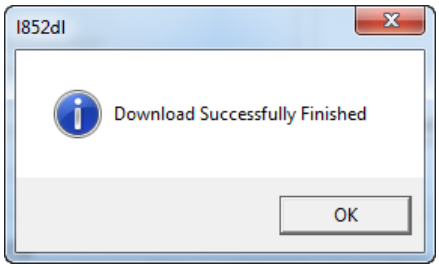


Abbildung 159: Erfolgreiche Aktualisierung der Firmware.

14 Fehleranalyse

14.1 LonMaker liefert eine Fehlermeldung beim Kommissionieren des L-IP

Problem

LonMaker zeigt eine Fehlermeldung beim Kommissionieren des L-IP wie in Abbildung 160 dargestellt.

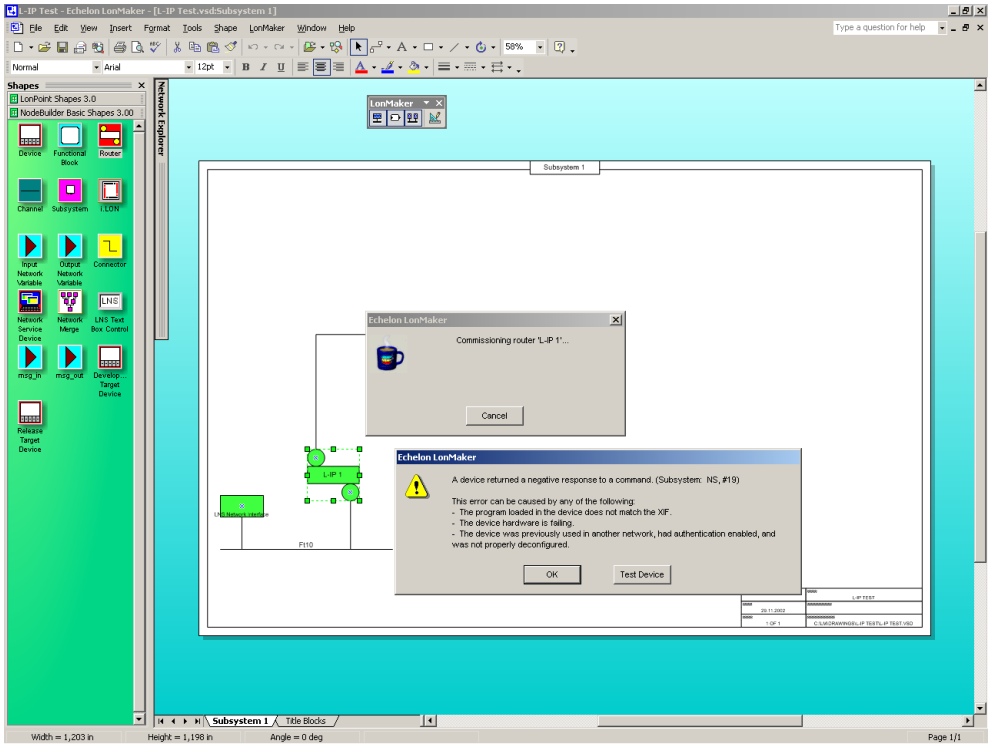


Abbildung 160: LonMaker kann den L-IP Router nicht kommissionieren.

Erklärung

Der L-IP ist nicht als CEA-709 Configured Router konfiguriert.

Lösung

Bitte stellen Sie sicher, dass die DIP-Schalter gemäß Abbildung 89 als konfigurierter Router eingestellt sind und starten Sie den L-IP neu. Möchten Sie den L-IP im Switch-Modus betreiben, dürfen Sie den L-IP nicht kommissionieren.

Falls das Problem weiterhin besteht, kontaktieren Sie bitte LOYTEC Support (Abschnitt 14.8).

14.2 Paketweiterleitung schlägt fehlt wenn Channel-Timeout aktiv ist

Problem

Der L-IP leitet keine Pakete weiter, wenn ein Channel-Timeout mit Wert >0ms angegeben wird.

Erklärung

Wahrscheinlich sind die Uhren in den L-IPs nicht synchronisiert und die Detektiereinheit von veralteten Paketen verwirft die Pakete, die von anderen L-IPs empfangen werden.

Lösung

Stellen Sie sicher, dass ein korrekter Wert für das Channel-Timeout gemäß Tabelle 6 eingegeben wurde und dass zumindest ein SNTP-Zeitserver für den CN/IP-Kanal angegeben wurde. Wird der L-IP hinter einer Firewall verwendet, stellen Sie sicher, dass die Firewall nicht die SNTP-Anfragen auf Port 123 blockiert.

14.3 Default Gateway Adresse ist falsch

Problem

Der L-IP meldet den Fehler “Can’t set default route:” während des Startvorganges.

```
LOYTEC electronics GmbH
www.loytec.com

Testing Board ID (0E)                                    Passed
Testing RAM                                              Passed
Testing boot loader                                      Passed
Testing fallback image                                   Passed
Testing primary image                                    Passed
Testing Flash                                            Passed

Loading primary image                                    Passed

Starting application                                     Passed

Port 1 detected (FT-10)                                  Passed

Can’t set default route: Network is unreachable
Starting TCP/IP networking (Timeout)                     Failed
```

Erklärung

Die Default-Gateway-Adresse ist auf eine falsche Adresse eingestellt oder auf eine Adresse die nicht existiert.

Lösung

Im Konfigurationsmenü “[5] IP configuration” wählen Sie den Punkt “[4] IP Gateway” und geben Sie eine gültige Gateway-Adresse ein. Auch wenn Sie kein Gateway verwenden, müssen Sie eine Gateway-Adresse für dieses Subnet angeben.

z. B. IP-Adresse: 192.168.1.34 => Gateway Adresse: 192.168.1.1.

14.4 TP-1250 Port funktioniert nicht

Problem

Nachrichten am TP-1250-Port werden nicht weitergeleitet.

Erklärung

Dieses Problem kann seine Ursache in dem gleichzeitigen Betrieb von Geräten mit ein- und solchen mit ausgeschaltetem Backbone-Modus im selben Netzwerksegment haben.

Lösung

Wenn der TP-1250-Kanal im Backbone-Modus verwendet werden soll, vergewissern Sie sich, dass alle an diesem Kanal angeschlossenen Geräte den Backbone-Modus aktiviert haben und bei jedem L-IP oder L-Switch eine eindeutige Geräte-ID konfiguriert wurde.

Falls der TP-1250-Kanal nicht im Backbone-Modus betrieben werden soll, vergewissern Sie sich, dass bei allen an diesem Kanal angeschlossenen L-IP- oder L-Switch-Geräten der Backbone-Modus ausgeschaltet ist.

14.5 CEA-709 Activity LED blinkt rot

Problem

Die CEA-709 Activity LED blinkt bei Verkehr am Netzwerk rot.

Erklärung

Der L-IP verfügt über eine eingebaute Netzwerkdiagnosefunktion (siehe Abschnitt 6.4.10). Sobald der L-IP ein potentielles Problem in einem angeschlossenen Netzwerksegment erkennt, blinkt die entsprechende Port-LED rot.

Lösung

Meistens ist die Ursache für dieses Verhalten ein Verkabelungsproblem oder ein zu hoher Netzwerkverkehr. Kontrollieren Sie Verkabelung und Netzwerkabschluss des betreffenden Ports. Konnten Sie bei der Verkabelung keinen Fehler entdecken, empfiehlt LOYTEC die Verwendung eines Protokollanalysators (z.B. LPA von LOYTEC) oder einer Netzwerkdiagnosesoftware (z.B. LOYTECs LSD-Tool oder Echelons Nodeutil), um die Ursache des Problems zu finden.

14.6 Die CEA-709 Activity LED und die Status LED blinken rot

Problem

Die CEA-709 Activity LED und die Status LED blinken ca. einmal pro Sekunde rot und der L-IP leitet keine Nachrichten weiter.

Erklärung

Der Grund für dieses Verhalten ist, dass das primäre L-IP-Firmware-Image fehlerhaft ist und daher das Fall-Back-Image gestartet wurde (siehe Abschnitt 7). Dieses Firmware-Image enthält keine Funktionalität zur Weiterleitung von Nachrichten. Es erlaubt lediglich, ein neues primäres L-IP-Firmware-Image zu übertragen und zu installieren.

Lösung

Wenn dieses Problem durch ein fehlgeschlagenes Firmware-Update hervorgerufen wurde, versuchen Sie die Firmware erneut zu aktualisieren.

Falls kein Firmware-Update vorgenommen wurde, wenden Sie sich bitte an den LOYTEC Support (Abschnitt 14.8).

14.7 IP-852 Datenverkehr kann am gesamten geswitchten IP Netzwerk gesehen werden

Problem

In einer Anlage, bei der CNIP-Router Daten nur in eine Richtung senden (Unacknowledged Services), werden vom empfangenden CNIP-Router keine Ethernetpakete ausgesendet. In diesem Fall vergessen Ethernet Switches nach einiger Zeit die MAC Adresse dieses CNIP Routers und leiten sämtliche Ethernetpakete mit dieser MAC Adresse an alle Ports weiter. Der Datenverkehr ist somit auf allen Ports sichtbar, was meist nicht gewünscht ist. Dieser Alterungsmechanismus für die MAC Adresse wird von vielen Ethernet Switches angewendet.

Erklärung

Ethernet Switches verwenden einen Alterungsmechanismus, um MAC Adressen im Gerät zu verwalten. Nach einiger Zeit altern diese MAC Adressen aus und müssen neu gelernt werden, andernfalls werden diese Datenpakete an alle Ports weitergeleitet.

Lösung

Please activate the keep alive function on the configuration server to establish two-way communication with the CNIP router.

14.8 Technischer Support

LOYTEC bietet für die L-IP-Produktserie deutschsprachigen Support per Telefon und E-Mail. Wenn keiner der obigen Lösungsansätze Ihr Problem behebt, kontaktieren Sie uns bitte unter der folgenden Adresse:

Delta Intelligent Building Technologies (Europe) GmbH
Blumengasse 35
A-1170 Wien
Österreich

E-Mail : ***support@loytec.com***
Web : ***https://www.loytec.com***
Tel : ***+43/1/4020805-100***

14.9 Paketaufzeichnung

14.9.1 Konfiguration der Remote-Paketaufzeichnung

Die Remote-Paketaufzeichnung kann Pakete auf dem Ethernet-Port aufzeichnen. Um das Feature für Remote Packet Capture zu aktivieren, gehen Sie zum Reiter **Ethernet** in der Port-Konfiguration und setzen den Haken **Remote packet capture** wie in Abbildung 161 gezeigt.

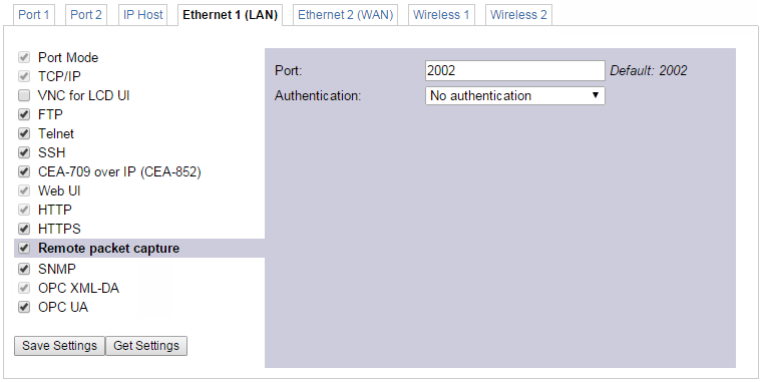


Abbildung 161: Remote packet capture in der Portkonfiguration.

Die Standardeinstellung für den Port kann bei Bedarf geändert werden. Normalerweise genügt jedoch die Standardeinstellung. Wenn **No authentication** ausgewählt ist, erlaubt das Gerät eingehende Capture-Verbindungen ohne weitere Angaben. Wenn **Username and Password** ausgewählt wird, müssen im Client von Wireshark gültige Angaben gemacht werden, bevor eine Capture-Sitzung gestartet werden kann. Beachten Sie dabei bitte, dass als Benutzer nur **admin** und **operator** erlaubt sind, wenn diese Methode ausgewählt wurde.

Klicken Sie auf den Knopf **Save Settings**, um die Konfiguration zu speichern. Die Einstellung wird sofort übernommen und ein Neustart des Geräts ist nicht erforderlich. Das Remote Capture kann auch wieder ohne Neustart deaktiviert werden.

14.9.2 Aktivieren einer lokalen Aufzeichnung

Das Gerät bietet auch eine Methode zur lokalen Aufzeichnung an. Damit zeichnet das Gerät Pakete lokal in einem internen Ringspeicher auf. Dieser kann dann vom Web-Interface heruntergeladen werden. Um zu verifizieren, ob das Gerät richtig konfiguriert ist, gehen Sie am Web-Interface zum Menü **Statistics → Packet capture** wie in Abbildung 162 gezeigt.

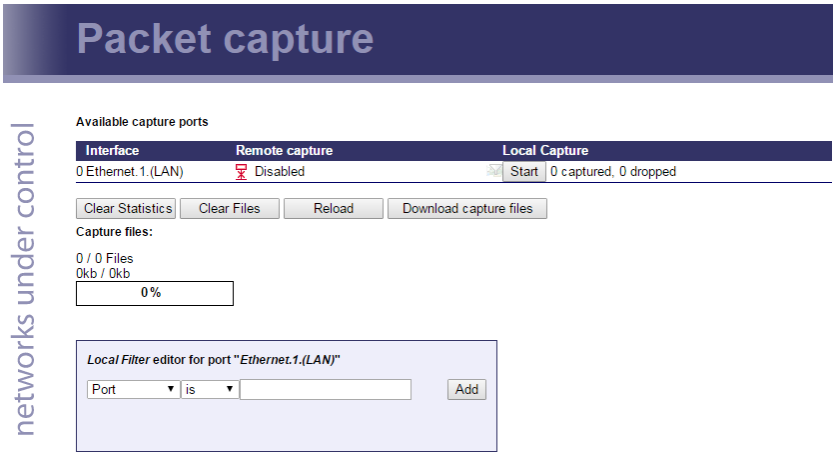


Abbildung 162: Statistiken zur Paketaufzeichnung.

Um den Offline Capture ohne angeschlossenem Wireshark auf dem Gerät zu starten, setzen Sie bitte den Haken **Local Capture**. Das Gerät startet dann die Aufzeichnung und speichert die Pakete in einem Ringspeicher ab. Die Log-Datei kann über den Knopf **Download capture files** heruntergeladen werden. Das speichert ein ZIP-Archiv der Aufzeichnung auf die lokale Festplatte ab. Die Aufzeichnungsdateien können durch Drücken des Knopfs **Clear Files** geleert werden. Nach einem Neustart gehen alle lokalen Aufzeichnungen verloren.

Für die lokale Ethernet-Paketaufzeichnung können zusätzliche Capture-Filter definiert werden, um die Menge an aufgezeichneten Paketen auf jene von Interesse einzuschränken.

Wählen Sie dazu die Zeile des Ethernet-Ports an und geben Sie im unteren Bereich der Seite eine Filterbedingung ein. Dann drücken Sie **Add** und geben weitere Filter ein. Schließlich drücken Sie den Knopf **Save Filters**, um die definierten lokalen Filter zu speichern und zu aktivieren. Abbildung 163 zeigt ein Beispiel, um auf Pakete mit der IP-Adresse 192.168.24.100 zu filtern.

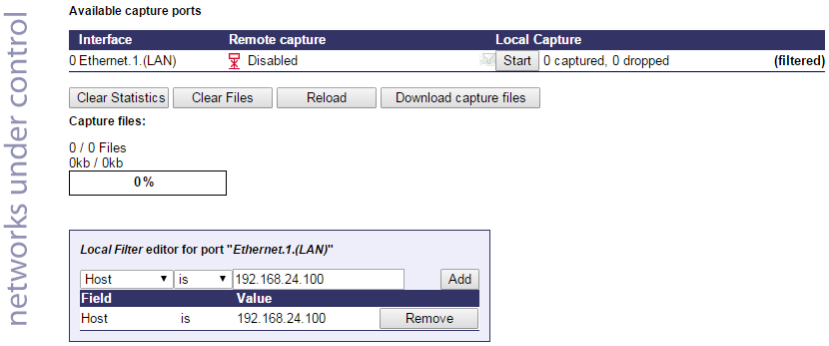


Abbildung 163: Hinzufügen eines lokalen Ethernet Capture-Filters.

14.9.3 Wireshark Remote-Aufzeichnung

Die Remote-Aufzeichnung benötigt zumindest einen Wireshark 1.6.11 mit WinPCAP 4.1.2. Bitte aktualisieren Sie ihre Wireshark-Installation auf diese oder eine neuere Version.

Hinzufügen eines Remote Capture Port

1. Öffnen Sie Wireshark und wählen Sie das Menü **Capture → Options…** . Das öffnet den Dialog **Capture Options** wie in Abbildung 164 dargestellt.

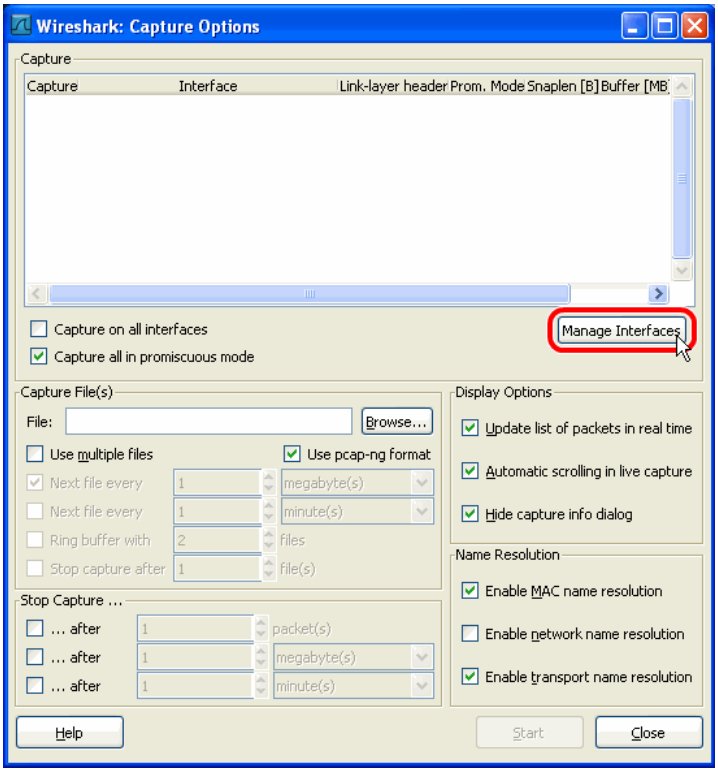


Abbildung 164: Wireshark Capture Options Dialog.

2. Klicken Sie auf den Knopf **Manage Interfaces**, um den Dialog **Add new interfaces** zu öffnen.

3. Wählen Sie den Reiter **Remote Interfaces** und klicken Sie **Add** wie in Abbildung 165 gezeigt wird.

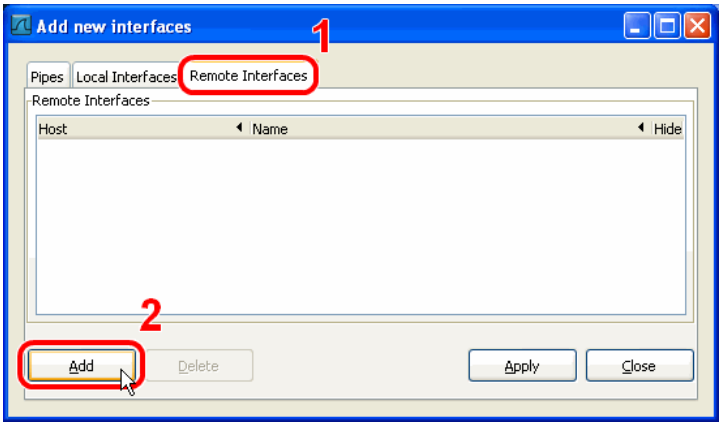


Abbildung 165: Wireshark Add New Interfaces Dialog.

4. Machen Sie dort die Einstellungen für **Host** und **Port** (Standard ist '2002') und geben Sie **Username** und **Password** in die entsprechenden Felder ein, falls **Password authentication** erfordert wird (siehe Abbildung 166).

5. Beachten Sie bitte, dass sich nur die Benutzer **admin** und **operator** verbinden können.

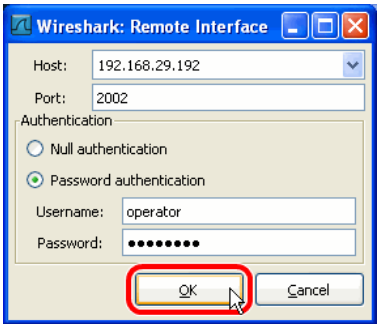


Abbildung 166: Wireshark Remote Interface Dialog.

6. Klicken Sie auf **OK**, um die Interface-Liste vom Gerät zu laden.

7. Wenn die Verbindung zum Gerät erfolgreich aufgebaut wurde, wird die Liste **Remote Interfaces** befüllt und enthält die Information über alle am Gerät verfügbaren Capture Ports wie in Abbildung 167 gezeigt.

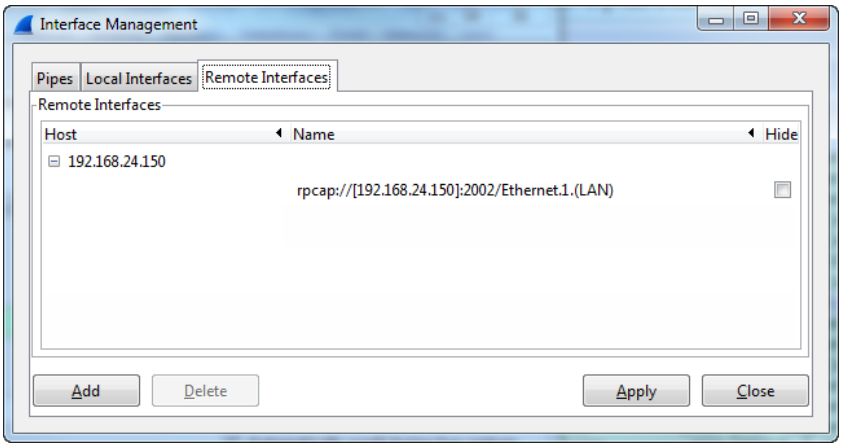


Abbildung 167: Neues Interface in Wireshark.

8. Schließen Sie die Dialoge **Add new interfaces** und **Capture Options** und kehren Sie ins Hauptfenster zurück.

To Start a Remote Capture

1. Wählen Sie im Hauptfenster das erzeugte Interface aus der Liste aus. Es ist mit ‚Raw Ethernet traffic' für Ethernet-Aufzeichnung und ‚SNAP encapsulated BACnet MS/TP traffic' für MS/TP-Aufzeichnung benannt.

2. Klicken Sie den Knopf **Start** wie in Abbildung 168 dargestellt.

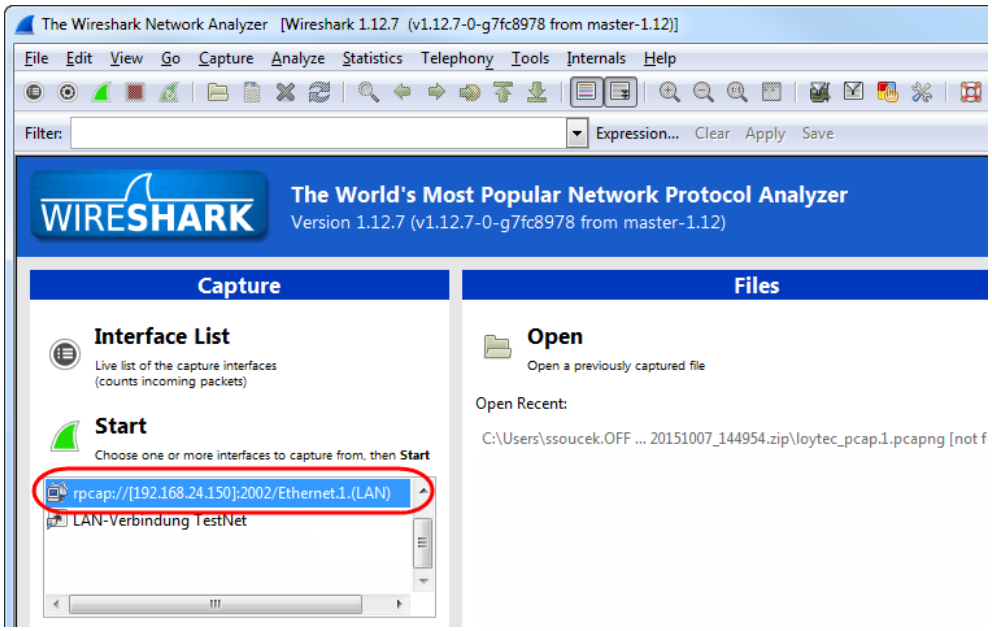


Abbildung 168: Starten einer Remote-Aufzeichnung in Wireshark.

3. Wireshark versucht nun die Verbindung zum Gerät aufzubauen. Wenn das funktioniert, startet Wireshark mit der Anzeige der Pakete. Ein Beispiel dazu ist in Abbildung 169 gezeigt.

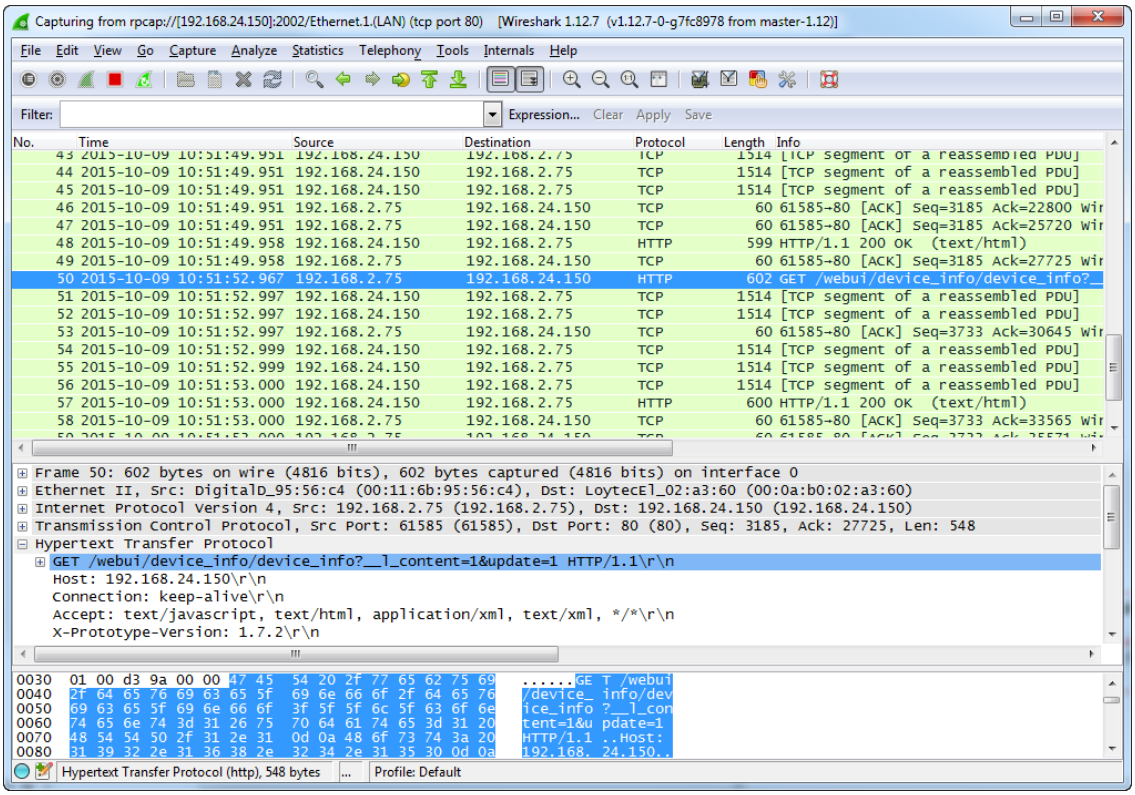


Abbildung 169: Beispiel für eine Ethernet Remote-Aufzeichnung im Betrieb.

15 Anwendungshinweise

Bitte beachten Sie die Anwendungshinweise aus Tabelle 8, um weiterführende Informationen zur Verwendung des L-IP in unterschiedlichen Anwendungsbereichen zu erfahren.

Anwendungshinweis	Thema
AN002G LSD Tool	Dieses Dokument beschreibt die Verwendung des LSD-Tools mit den L-Switch und L-IP Geräten.
AN003G L-IP und LNS	Dieses Dokument beschreibt, wie der L-IP mit LNS-basierenden Netzwerkmanagement-Tools zusammenarbeitet.
AN005G L-IP Backbone	Dieses Dokument zeigt, wie L-Switch Geräte über einen L-IP (Ethernet) Backbone verbunden werden können.
AN007G Netzwerkinfrastruktur	Dieses Dokument beschreibt an Hand von Beispielen, wie LOYTEC Infrastrukturkomponenten (L-Switch, L-IP, L-Proxy und NIC) zusammen mit LOYTEC Netzwerkadaptern eingesetzt werden. Es erklärt weiters die unterschiedlichen Betriebsarten der Geräte und welche Betriebsart fuer welche Anwendung geeignet ist.

Tabelle 8: Anwendungshinweise für den L-IP.

16 Security-Leitfaden

Dieser Abschnitt ist ein Leitfaden, der Informationen zur Security beim Betrieb des Produkts in IT-Netzwerken enthält. Die Informationen beziehen sich auf die aktuelle Firmware-Version und die Anweisungen, die in den vorhergehenden Kapiteln des Benutzerhandbuchs gefunden werden können.

16.1 Installationshinweise

Verwenden Sie zur Inbetriebnahme des Geräts das Web-Interface:

- Nehmen Sie die Einstellungen zum Betrieb des Geräts und der Kommunikations-protokolle vor, wie im Abschnitt 5.2 und 7.3 beschrieben. Bei der Konfiguration über das Web-Interface verwenden Sie die https:// URL.
- Ändern Sie das Standard-Admin-Passwort auf ein sicheres Passwort wie in Abschnitt 7.1 beschrieben. Mit Firmware 8.4.0 werden starke Passworte erzwungen.
- Deaktivieren Sie den HTTP-Service in der Port-Konfiguration wie in Abschnitt 7.3.3 beschrieben.
- Erstellen Sie ein eigenes HTTPS Server-Zertifikat wie in Abschnitt 7.4.2 beschrieben.
- Legen Sie ein Passwort für den Benutzer „guest“ fest oder deaktivieren sie dieses Konto, um Informationen der Geräteinfoseite vor ungewollter Offenlegung zu schützen.

16.2 Firmware

Das Gerät ist mit einem Stück Software ausgestattet. Diese ist durch das Firmware-Image und die zugehörige Firmware Version gekennzeichnet. Die Firmware wird als ladbare Datei vertrieben. Das Gerät kann durch Aufspielen dieses Firmware Images aktualisiert werden, wie in Kapitel 13 beschrieben. Die Gerätefirmware wird von LOYTEC signiert und ihre Signaturintegrität wird überprüft, bevor das Upgrade zugelassen wird. Wenn die Signatur der Firmware nicht verifiziert werden kann, wird das Upgrade nicht durchgeführt und die Datei gelöscht.

Für alle L-IP Modelle existiert exakt ein und dasselbe Firmware-Image. Die Firmware hat eine eingebaute Auto-Detektierung, die die Feldbus-Ports erkennt, mit denen das Gerät ausgestattet ist. Sie fügt virtuelle Router auf einen internen Kanal hinzu. Für die Funktionalität macht dies keinen Unterschied, da die IP-Verbindung ebenfalls auf den internen Kanal aufgeschaltet ist.

Cyber-Security-Haftungsausschluss für Firmware-Upgrades

LOYTEC veröffentlicht regelmäßig Firmware-Updates, die Sicherheitslücken schließen. Wird ein Sicherheitsupdate nicht installiert, bleibt das Gerät bekannten und dokumentierten Sicherheitsbedrohungen ausgesetzt, was zu unbefugtem Zugriff auf das Gerät, zur Änderung oder Offenlegung von Konfigurations- und vertraulichen Benutzerdaten oder zur Unterbrechung des Gebäudeautomationsbetriebs führen kann. LOYTEC übernimmt keine Haftung für Sicherheitsvorfälle, Unfälle oder Ausfälle, die auf die Verwendung eines

Produkts zurückzuführen sind, für das verfügbare Sicherheitsupdates nicht installiert wurden. Es liegt in der ausdrücklichen Pflicht des Benutzers, Sicherheitsupdates unverzüglich nach deren Veröffentlichung durch LOYTEC zu installieren.

16.3 Ports

Dieser Abschnitt listet alle Ports auf, die vom Gerät benutzt werden können. Die Angaben für die Ports sind Standardeinstellungen für die jeweiligen Dienste. Wenn nicht anders angegeben, können diese Ports geändert werden.

Benötigte Ports:

- 1628 udp/tcp: Das ist der Port für den Datenaustausch über CEA-852 (LON über IP). Er ist für die primäre Produktfunktion und den Betrieb zum Datenaustausch zwischen Routern über das IP-Netzwerk erforderlich. Jedes Gerät muss diesen Port geöffnet haben. Der Port kann geändert werden
- 1629 udp/tcp: Das ist der Port für den CEA-852 Configuration Server. Es muss genau ein Gerät im System diesen Port geöffnet haben. Andere Geräte registrieren sich beim Configuration Server, um einen IP-852 Kanal zu formen. Der Port kann geändert werden.

Folgende optionale Ports, die für die primäre Produktfunktion nicht benötigt werden, können deaktiviert werden. Dies ist in den Anweisungen in Abschnitt 16.1 beschrieben:

- 21 tcp: This Dieser Port wird für den FTP-Server verwendet und ist in der Standard-einstellung geschlossen.
- 22 tcp: Dieser Port ist für den SSH-Server offen. Er kann geändert und geschlossen werden.
- 23 tcp: Dieser Port wird für den Telnet-Server verwendet und ist in der Standard-einstellung geschlossen.
- 80 tcp: Dieser Port ist für den Web-Server und den OPC XML-DA Server offen. Er kann geändert und geschlossen werden.
- 161 tcp: Dieser Port ist offen für den SNMP Server Der Port ist in der Standardeinstellung geschlossen. Der Port kann geändert werden.
- 443 tcp: Dieser Port ist offen für den sicheren Web Server über HTTPS und den OPC XML-DA Server. Er kann geschlossen werden.
- 2002 tcp: Dieser Port ist offen für das Wireshark Protokollanalysator Front-End. Der Port ist in der Standardeinstellung geschlossen. Der Port kann geändert werden.
- 4840 tcp: Dieser Port ist offen für den OPC UA Server. Der Port ist in der Standardeinstellung geschlossen. Der Port kann geändert werden.
- 5353 udp: Dieser Port ist geöffnet, um das Gerät über mDNS-Namen wie loytec.local zu finden. Dieser Port kann deaktiviert werden.
- 1900 udp: Dieser Port ist für den SSDP-Discovery-Dienst offen. Er kann nicht deaktiviert werden.
- 5900 tcp: Dieser Port ist offen für den VNC Server. Der Port ist in der Standard-einstellung geschlossen. Der Port kann geändert werden.

16.4 Dienste

Benötigte Dienste:

- CEA-852 (LON über IP): Dieser Dienst ist für die primäre Produktfunktion erforderlich. Der Dienst ist konform zum Standard ANSI/CEA-852-B.

Folgende optionale Dienste, die für die primäre Produktfunktion nicht benötigt werden, können deaktiviert werden Dies ist in den Anweisungen in Abschnitt 16.1 beschrieben:

- mDNS: Dieser Dienst dient dazu, das Gerät über Multicast-DNS zu finden und so die erste Kommunikation herzustellen. Dies ermöglicht die Verwendung von DNS-Namen wie loytec.local im Webbrowser. Dieser Dienst kann deaktiviert werden.
- HTTP: Web-Server. Dieser Dienst wird für die Web-basierende Konfigurationsschnittstelle benötigt. Das Web-Interface kann nach Abschluss der Inbetriebnahme deaktiviert werden.
- FTP und Telnet: Der FTP- und Telnet-Server werden für die Verbindung zum Gerät für Remote-Konfiguration (L-WEB), die Aktualisierung der Firmware und den Zugriff auf das Systemprotokoll verwendet. Diese Dienste sind in der Standardeinstellung nicht aktiviert.
- SSH: Dieser Dienst bietet sicheren Zugriff auf das Konsole-Menü über das IP-Netzwerk.
- HTTPS: Sicherer Web Server. Dieser Dienst bietet die sichere Web-basierdene Konfigurationsschnittstelle über HTTPS. Er wird für Remote-Konfiguration (L-WEB), die Aktualisierung der Firmware und den Zugriff auf das Systemprotokoll verwendet.
- VNC: Der VNC-Server kann für den Zugriff auf die LCD-Anzeige über das Netzwerk verwendet werden, wenn das Gerät darüber verfügt. Der Dienst ist in der Standardeinstellung nicht aktiviert.
- OPC XML-DA: Dieses Web-Service ermöglicht den Zugriff auf Datenpunkte über den OPC XML-DA Standard. Der Dienst ist in der Standardeinstellung nicht aktiviert.
- OPC UA: Dieses sichere Service ermöglicht den Zugriff auf Datenpunkte über den OPC UA Standard. Der Dienst ist in der Standardeinstellung nicht aktiviert.
- SNMP: SNMP Server. Dieser Dienst bietet Netzwerk-Management Informationen vom Gerät an, die von gebräuchlichen Werkzeugen der IT verwendet werden können. Der Dienst ist in der Standardeinstellung nicht aktiviert.
- Wireshark Front-End: Der Wireshark Protokollanalysator kann sich mit diesem Service auf das Gerät verbinden und Protokollaufzeichnungen online abholen. Der Dienst ist in der Standardeinstellung nicht aktiviert.

16.5 Upgrade auf stärkere Schlüssel

Die sicheren Dienste (HTTPS, SSH) setzen Zertifikate voraus, die der verbundene Client zur Authentifizierung des Geräts verwendet. Das ist besonders wichtig, um Man-In-The-Middle-Attacken zu verhindern. Das Gerät besitzt dazu ein vorinstalliertes Server-Zertifikat. Es empfiehlt sich ein Upgrade des vorinstallierten Zertifikats auf ein für das Gerät individualisiertes Zertifikat mit stärkerem Schlüssel.

- Server-Zertifikat (für HTTPS, OPC UA): Folgen Sie der Beschreibung im Abschnitt 7.4.2, um das vorinstallierte X.509 Zertifikat durch ein individuelles selbstsigniertes oder durch eine CA signiertes Zertifikat und stärkerem Schlüssel zu ersetzen.
- SSH Key Upgrade: Ist SSH aktiviert, empfiehlt es sich ein Upgrade auf einen stärkeren SSH-Schlüssel. Folgen Sie der Beschreibung im Abschnitt 7.3.16, um ein Upgrade auf einen RSA-Schlüssel mit 2048 Bits durchzuführen.

16.6 Protokoll und Audit

Das Gerät bietet ein Systemprotokoll, die über SSH oder den Web-Server ausgelesen werden kann. Das Systemprotokoll beinhaltet Informationen darüber, wann das Gerät gestartet hat und wann nennenswerte Kommunikationsfehler aufgetreten sind. Informationen zum User Log-On werden nicht aufgezeichnet, da die primäre Produktfunktion keine Benutzerverwaltung erfordert.

Protokollierte Ereignisse:

- Zeitpunkt des letzten Systemstarts des LOYTEC-Geräts.
- Zeitpunkt und Version der letzten Firmware-Aktualisierung.
- Zeitpunkt, wann die Konfiguration vom Gerät gelöscht oder das Gerät auf Werkseinstellungen zurückgesetzt wurde.
- Kommissionierung des CEA-709 Knoten/Router.
- Statische Fehler im Gerät oder der Konfiguration.
- Überlastsituationen als einmalige Protokolleinträge seit dem letzten Neustart.
- Nennenswerte Kommunikationsfehler bei ihrem Auftreten.
- Logins und Fehler beim Login.
- Fehlgeschlagene Versuche einer Firmware-Aktualisierung.

16.7 Netzwerkzugriff

Der Netzwerkzugriff kann durch Verwendung der 802.1X-Portauthentifizierung (ab Firmware 7.4.0) mit EAP-TLS, PEAP oder TTLS geschützt werden. Nicht verwendete Ethernet-Ports können deaktiviert werden.

16.8 Passwortschutz

Geräte bieten separate administrative (admin) und operative (operator) Benutzerkonten. Passworte werden nicht direkt gespeichert, sondern es wird ein starker, kryptografischer Hash gespeichert (salted SHA256). Die Geräteanmeldung wird durch eine Anmeldefalle geschützt, die die Anmeldung nach zehn aufeinanderfolgenden, fehlgeschlagenen Anmeldeversuchen mit unterschiedlichen Passworten für 10 Sekunden blockiert, um sich vor Brute-Force-Kennwortangriffen zu schützen. Die anfängliche Kennworteinstellung wird mit starkem Passwort erzwungen. Ohne Festlegung des initialen Passworts ist die Gerätefunktionalität gesperrt. Passwörter können bis zu 64 Zeichen lang sein und alle druckbaren UTF-8-Zeichen enthalten.

Um die Verwendung des Administratorkennworts zu schützen, kann der Administrator zusätzliche Benutzerkonten mit einer Administratorrolle erstellen. Diese zusätzlichen Benutzerkonten können nach Bedarf deaktiviert werden. Benutzernamen dürfen maximal 32 Zeichen lang sein. Die integrierten Benutzerkonten können deaktiviert werden, wenn benutzerdefinierte Benutzerkonten mit diesen Rollen erstellt wurden.

16.9 Verschlüsselung im Speicher

Für den Betrieb erforderliche Client-Anmeldeinformationen (z.B. E-Mail-Client) werden verschlüsselt mit AES256-CBC und Nonce gespeichert. Der geheime Schlüssel dafür ist an das Gerät gebunden und kann nicht vom Gerät abgerufen oder ausgelesen werden.

Anmeldeinformationen können verschlüsselt mit einem Projektpasswort und PBKDF-2 exportiert oder importiert werden.

16.10Sichere Entsorgung und Außerbetriebnahme

Bevor Sie ein LOYTEC-Gerät entsorgen, weiterverkaufen oder zurückgeben, müssen Sie alle geschützten Informationswerte (Kommunikations- und Sicherheitskonfiguration, benutzerdefinierte Werte, personenbezogene Daten, Authentifizierungsdaten und kryptografische Schlüssel) löschen, um deren Offenlegung zu verhindern. Um die Nutzung eines LOYTEC-Geräts sicher zu beenden:

1. Sichern Sie die erforderliche Konfiguration (Gerätesicherung durch Projektpasswort geschützt).

2. Führen Sie einen Werksreset / Zurücksetzen auf Standardwerte durch (siehe LOYTEC Geräte Benutzerhandbuch [1]). Dadurch werden alle Benutzerdaten, benutzerdefinierten Werte und Anmeldedaten gelöscht. Die Firmware-Version bleibt erhalten.

3. Entfernen Sie gegebenenfalls die SD-Karte oder Wechselspeichermedien und vernichten Sie diese physisch, oder löschen Sie sie sicher.

4. Entfernen Sie das Gerät aus jedem VPN-, 802.1X- oder Management-System (widerrufen Sie dessen Zertifikate und Anmeldedaten in diesen Systemen).

5. Entsorgen Sie Elektroschrott gemäß den örtlichen Vorschriften (z. B. WEEE in der EU).

Wichtig!	*Geräte, die verkauft oder entsorgt werden, ohne dass die geschützten Informationswerte wie beschrieben gelöscht wurden, können Konfigurationsdaten, Anmeldedaten und Projektdaten der Gebäudeautomation dem neuen Besitzer des Geräts offenlegen.*

16.11Informationsrichtlinie

LOYTEC verfolgt eine Richtlinie zur Meldung, Dokumentation und Information über potenzielle Sicherheitslücken und Sicherheitshinweise:

1) Auf der LOYTEC-Website wird die Anmeldung für einen Mailinglisten-Newsletter angeboten, um sicherheitsrelevante Informationen zeitnah zu erhalten.
2) Auf der LOYTEC-Website finden Sie ein Formular zur Meldung potenzieller Sicherheitslücken in Bezug auf LOYTEC-Produkte. Meldungen von Vorfällen können auch per E-Mail an security@loytec.com gesendet werden. Sie erhalten eine Antwort mit einer nachverfolgbaren Kennung. LOYTEC akzeptiert Sicherheitsberichte, die den gängigen Richtlinien für verantwortungsvolle Offenlegung entsprechen und technische Informationen zur Reproduktion der Probleme, Exploit-Skripte oder andere Informationen enthalten, die es ermöglichen, kritische Sicherheitsprobleme zu identifizieren und zu beheben.
3) LOYTEC verpflichtet sich, Sicherheitsfixes für Zero-Day-Exploits innerhalb von 96 Stunden nach Kenntniserlangung bereitzustellen. Alle weiteren, sicherheitsrelevanten Fixes werden innerhalb von 30 Tagen mit dem nächsten Firmware-Patch bereitgestellt.

17 Spezifikationen

17.1 Technische Spezifikationen

17.1.1 LIP-xxECRB

Betriebsspannung	12-35 VDC oder 12-24 VAC ±10%
Leistungsaufnahme	typ. 3 W
Einschaltstrom	bis 950 mA @ 24 VAC
Betriebstemperatur (Umgebung)	+0 °C bis +50 °C
Lagertemperatur	–10 °C bis +60 °C
Rel. Luftfeuchtigkeit im Betrieb	10 bis 90% RH @ 50 °C
Rel. Luftfeuchtigkeit in Lagerung	10 bis 90% RH @ 50°C
Gehäuse	Installationsgehäuse 107 mm breit, DIN 43 880
Schutzart	IP 40 (Gehäuse); IP 20 (Schraubklemmen)
Montage	DIN Hutschiene (EN 50 022) oder Wandmontage

17.1.2 LIP-3ECTC, LIP-33ECTC, LIP-13ECTC

Betriebsspannung	20-30 VAC/VDC
Leistungsaufnahme	typ. 3 W
Einschaltstrom	bis 950 mA @ 24 VAC
Betriebstemperatur (Umgebung)	+0 °C bis +50 °C
Lagertemperatur	–10 °C bis +60 °C
Rel. Luftfeuchtigkeit im Betrieb	10 bis 90% RH @ 50°C
Rel. Luftfeuchtigkeit in Lagerung	10 bis 90% RH @ 50°C
Gehäuse	Installationsgehäuse 107 mm breit, DIN 43 880
Schutzart	IP 40 (Gehäuse); IP 20 (Schraubklemmen)
Montage	DIN Hutschiene (EN 50 022) oder Wandmontage

17.1.3 LIP-3333ECTC

Betriebsspannung	20-30 VAC/VDC
Leistungsaufnahme	typ. 3 W
Einschaltstrom	bis 950 mA @ 24 VAC
Betriebstemperatur (Umgebung)	+0 °C bis +50 °C
Lagertemperatur	–10 °C bis +60 °C
Rel. Luftfeuchtigkeit im Betrieb	10 bis 90% RH @ 50°C
Rel. Luftfeuchtigkeit in Lagerung	10 bis 90% RH @ 50°C
Gehäuse	Installationsgehäuse 159 mm breit, DIN 43 880
Schutzart	IP 40 (Gehäuse); IP 20 (Schraubklemmen)
Montage	DIN Hutschiene (EN 50 022) oder Wandmontage

17.2 FCC Hinweis

Dieses Gerät wurde getestet und entspricht den Beschränkungen für ein Digitalgerät der Klasse B entsprechend Abschnitt 2 und 15 der FCC. Bestimmungen. Diese Beschränkungen dienen einem angemessenen Schutz von nachteiligen Störungen, sofern das Gerät in einer handelsüblichen Umgebung betrieben wird. Dieses Gerät erzeugt, nutzt und strahlt Funk-Frequenzenergie ab und kann, sofern es nicht in Übereinstimmung mit der Bedienungsanleitung installiert und betrieben wird, zu nachteiligen Störungen von Funkkommunikationen führen. Der Betrieb dieses Geräts in einem Wohnbereich führt möglicherweise zu nachteiligen Störungen, in diesem Fall hat der Nutzer auf seine Kosten für eine Behebung der Störungen zu sorgen.

17.3 CE Hinweis

Dies ist ein Klasse B Produkt. In einer häuslichen Umgebung kann das Gerät Funkstörungen verursachen; in diesem Fall ergreifen Sie bitte angemessene Maßnahmen.

18 Quellenangabe

[1] LOYTEC Geräte Benutzerhandbuch 8.6, Delta IBT (Europe) GmbH, Dokument № 88086614, August 2026.

19 Versionsverzeichnis

Date	Version	Author	Description
2002-07-11	1.0	DL	Initial revision V1.0
2003-01-17	1.1	DL	Added menu item 9 (device statistics) in Section 4.10 Improved behavior of cnip LED in Section 3.4.7 Added automatic IP connection keep-alive in Section 4.6.8
2003-05-09	2.0	DL	Add Section 2.3 IP Configuration for Client Device via Web-Interface Add Section 4.4.3 Option 8 – Webserver Add Section 4.4.4 Option 9 - Change Web server Password Changed menu in Section 4.5 CEA-709 Configuration Menu Rewrite Section 4.5.1 and Section 4.5.2. Add Section 4.7.10 Option 9 - Location string Add Section 4.8.7 Option 7 - Auto members support Add Section 4.8.8 Option 8 - Roaming members support Add Section 4.8.15 Option s - Show device statistics Add Section 4.8.17 Option r - Recontact devices & list channel members Add new device states to Tabelle 14 Add flags to Abbildung 35: List all CN/IP channel members. Add Chapter 5 Web Interface Add Section 4.4.2.3 Option 3 - Set router configuration according to DIP switch Add Section 7.9 Remote LPA Operation Rewrite Section 7.11.3 DHCP
2003-09-15	2.1	DL	Added note about PC NTP client to Section 7.10.1 Add Section 11.7 IP-852 traffic may flood the entire switched IP network Corrected information on controlling RS-485 bit-rate auto-detection with DIP switch, see Section 3.6 Add route command starting with firmware version 2.1 in Section 2.3 and Section 5.1. Add Section 4.10.6 Option 6 - Enhanced Communications Test Add Enhanced Communications Test to Section 5.4
2004-04-15	2.2	JB	Updated for L-IP 2.2
2004-09-21	3.0	STS	Added extended NAT, multi-cast, Auto-NAT, new enhanced communications test, new channel list in Web, i.LON 600. Corrected terminals 25, 26.
2005-04-19	4.3	STS	Updated manual for multi-port L-IP.
2005-09-22	4.4	JB	Updated manual for L-IP Redundant
2006-06-27	4.5	JB	Updated manual for LIP-xxxxECTB
2012-09-28	6.0	JB	Aktualisiert für Firmware Version 6.0. Information über alte L-IP Produkte entfernt. Bilder für Gehäuse aktualisiert. Neues Design des Benutzerhandbuchs. Neues Kapitel Security-Leitfaden. Kleinere Korrekturen.
2013-08-22	6.0	STS	Deutsches Benutzerhandbuch zu 6.0.
2015-10-09	6.1	STS	Aktualisiert für Firmware Version 6.1. Neuer Abschnitt 1.2 L-IP Modelle. Neues Kapitel 2 Was ist neu im L-IP. Kapitel 4 bezieht sich auf die Installationsblätter, Abschnitte Anschlüsse, Gehäuse, Produkt-Labels, DIP-Schalter gelöscht. Neuer Abschnitt 3.2.3 Konfiguration über das LCD-Display. Neuer Abschnitt 4.6 LCD-Anzeige und Dreh-/Drückrad. Neuer Abschnitt 6.2.5 Verwenden mehrerer IP-Ports. Neuer Abschnitt 6.2.6 IP Host-Konfiguration. Neuer Abschnitt 6.2.7 WLAN-Konfiguration. Neuer Abschnitt 6.2.8 VNC-Konfiguration. Neuer Abschnitt 6.2.14 Zertifikate verwalten. Neuer Abschnitt 6.2.15 Firmware. Neuer Abschnitt 6.2.16 SNMP. Neuer Abschnitt 6.2.17 Dokumentation. Aktualisiert 6.3.1 System Log. Neuer Abschnitt 6.4 Dokumentation. Neuer Abschnitt 10.1 SNMP Interface. Neuer Abschnitt 11.4 Redundante Ethernet-Verkabelung. Neuer Abschnitt 11.5 WLAN. Neuer Abschnitt 12.1 Firmware Update über das Web Interface. Neuer Abschnitt 13.9 Paketaufzeichnung. Aktualisiertes Kapitel 15 Security-Leitfaden. Kapitel Firmware Versionen gelöscht.

2018-08-08	6.4	STS	Aktualisiert für Firmware Version 6.4. Abschnitt 6.2.1 Sprachauswahl beschrieben. Neuer Abschnitt 6.2.14 SSH-Server-Konfiguration. Aktualisierter Abschnitt 6.2.15 Zertifikat-Verwaltung. Abschnitt 6.2.16 Backup vor dem Firmware-Upgrade dokumentiert. Neuer Abschnitt 6.5.1 Sicherer Neustart. Aktualisierung des Kapitel 15 Security-Leitfaden.
2019-09-25	7.0	STS	Aktualisiert für Firmware Version 7.0. Neuer Abschnitt 6.2.19 VPN-Konfiguration. Aktualisierung des Kapitel 15 Security-Leitfaden.
2021-04-26	7.4	STS	Aktualisiert für Firmware Version 7.4. Kapitel zum Konsole-Interface entfernt. Kapitel 7: Neu organisiert, um der neuen Menüstruktur zu entsprechen. Abschnitt 7.1.1: Aktualisiertes Geräte-Setup und Kennwortdurchsetzung. Abschnitt 7.3.5: 802.1X-Portauthentifizierung hinzugefügt. Abschnitt 7.3.7: dynamisches DNS hinzugefügt. Abschnitt 7.3.18: Beschreibung der Registerkarte VPN hinzugefügt. Abschnitt 7.3.19: LTE-Konfiguration hinzugefügt. Aktualisiertes Kapitel 16 Security-Leitfaden.
2023-03-30	8.0	STS	Aktualisiert für Firmware Version 8.0. Abschnitt 7.3.8 + 7.3.9: Aktualisierungen der WLAN-Reiter (Client, AP, Mesh). Abschnitt 7.3.16 EC-Schlüssel zum SSH-Server hinzugefügt. Abschnitt 7.4.2 EC-Schlüsseloption zur Zertifikatsverwaltung hinzugefügt. Aktualisiertes Kapitel 16 Security-Leitfaden.
2024-01-05	8.2	STS	Aktualisiert für Firmware Version 8.2.
2024-06-15	8.2.8	STS	Aktualisiert für Firmware Version 8.2.8. Modell LIP-13ECTC hinzugefügt. Neuer Abschnitt 5.4: Als LON-Router-Drop-in-Ersatz konfigurieren. Neuer Abschnitt 6.6.4: LCD-Menü im Router-Modus. Neuer Abschnitt 9.3: L-IP fungiert als L-Switch.
2025-06-16	8.4.0	STS	Aktualisiert für Firmware Version 8.4.0. Methode mit ‚loytec.local' in Abschnitt 5.2.1 hinzugefügt. Aktualisierung des Kapitel 16 Security-Leitfaden.
2026-08-30	8.6	STS	Firmenname im gesamten Handbuch aktualisiert. Aktualisiert für Firmware Version 8.6.0. Versorgungsspannungsbereich aktualisiert auf 20-30 VAC/VDC. Kapitel 16 (Security-Leitfaden): Cyber-Security-Haftungsausschluss für Firmware-Upgrades zu Abschnitt 16.2 (Firmware) hinzugefügt, SSDP-Port und OPC XML-DA in Abschnitt 16.3 (Ports) und Abschnitt 16.4 (Dienste) ergänzt sowie neuer Abschnitt „Sichere Entsorgung und Außerbetriebnahme" vor Abschnitt 16.11 (Informationsrichtlinie) eingefügt. Kapitel 18: Quellenangabe hinzugefügt.