1 Einführung

Dieses Dokument beschreibt anhand von Beispielszenarien den Einsatz von LOYTEC Netzwerkinfrastrukturprodukten (L-Switch Router, L-Switch^{XP} Router, L-IP Router und L-Proxy Gateway) und LOYTEC Netzwerkschnittstellenkarten (NICs) zum Aufbau leistungsfähiger, verlässlicher Netzwerke. In diesem Zusammenhang werden verschiedene Betriebsarten beschrieben und auch auf Diagnose- und Analysemöglichkeiten im Netzwerk wird eingegangen.

2 Gründe für die Strukturierung von Netzwerken

Zusammen mit der Größe von Netzwerken steigt auch deren Komplexität. Es gibt eine Reihe von technischen, aber auch praktische Gründe für die Strukturierung von Netzwerken:

- Beschränkung der Knotenanzahl pro Kanal: Die Spezifikation der unterschiedlichen Transceiver-Typen [2] limitieren die maximal erlaubte Anzahl von Knoten, die an einzelnen Kanälen angeschlossen werden dürfen. Beispielsweise beträgt die für TP/FT-10 Kanäle maximal zulässige Anzahl von Knoten pro Netzwerksegment 64. Übersteigt die Anzahl der am Kanal benötigten Knoten diesen Wert, so müssen Netzwerkinfrastrukturprodukte eingesetzt werden (siehe Tabelle 1).

- Maximal zulässige Kabellänge: Die Transceiver- und Kabel-Spezifikationen beschränken die maximal zulässige Kabellänge pro Netzwerksegment. Die Maximallänge ist abhängig vom verwendeten Transceivertyp sowie von der Netzwerktopologie (Bus, Freie Topologie, siehe Tabelle 1).

- Verringerung der Busbelastung: Bei steigender Knotenanzahl nimmt meist auch die Menge an Daten zu, die zwischen den Knoten ausgetauscht werden. Router und Switches können zur Vermeidung einer Kanalüberlastung eingesetzt werden. Diese Komponenten filtern Datenpakete in Abhängigkeit der Zieladresse und reduzieren auf diese Weise die Kanalauslastung.

- Erhöhen der Zuverlässigkeit: Switches und Router können Rauschen und zerstörte Datenpakete (Datenpakete mit CRC Fehlern oder verfälschtem Inhalt) ausfiltern. Wenn ein Paket, z. B. durch Rauschen am Netzwerk verfälscht wird, wird dieses verworfen, anstatt es an das angeschlossene Netzwerksegment weiterzuleiten. Dies garantiert einen guten Gesamtzustand des Netzwerks, auch wenn Störungen in einzelnen Netzwerksegmenten auftreten.

- Bessere Wartbarkeit: In strukturierten Netzwerken können zu Wartungszwecken einzelne Segmente isoliert werden, um Arbeiten durchzuführen, ohne das übrige Netzwerk zu beeinträchtigen. Außerdem stellen LOYTECs L-IP Router eine Schnittstelle zur Verfügung, um mit dem LPA Protokollanalysator über einen IP-852 (Ethernet/IP) Kanal auf Netzwerksegmente hinter dem L-IP Router zugreifen zu können und diese Kanäle (TP/FT-10, TP/XF-1250, RS-485) zu analysieren. Da hier auf das IP-Protokoll aufgesetzt wird, kann der Zugriff auch über ein Intranet oder über das Internet erfolgen.

3 Elektrische Eigenschaften

3.1 Kanaltypen

Kanaltyp	Kabellängen und -typen	Knoten pro Segment
TP/FT-10 (Bus)	KAT5 Kabel 24AWG(0,5mm): 900m (max. Stichleitungslänge = 3m)	64 (128 für Link Power Transceiver)
TP/FT-10 (Freie Topologie)	KAT 5 Kabel 24AWG(0,5mm): 450m Max. Knoten-Knoten Abstand: 250m	64 (128 für Link Power Transceiver)
TP/XF-1250	Kat 4 Kabel 22AWG (0.65mm): Typ. 500m Worst Case 130m Max. Stickleitungslänge 0,3m	64 (0 bis +70°C) 32 (-20 bis+85°C) 20 (-40 bis +85°C) <=8 Geräte pro 16m Segment
IP-852	Ethernet 10BaseT	256

Tabelle 1: Standard-Transceiver und deren Spezifikation [1]

3.2 Terminierung

Voraussetzung für einen reibungslosen Betrieb von Netzwerken ist eine den Spezifikationen entsprechende Terminierung.

Hinweis: Bei Multiport-Geräten müssen alle Netzwerkanschlüsse – auch jene, die nicht benutzt werden – gemäß den Spezifikationen terminiert werden.

3.2.1 TP/XF-1250

Der TP/XF-1250 Kanal verwendet Übertrager zur galvanischen Trennung des Knotens vom Netzwerk. TP/XF-1250 Kanäle müssen in Bustopologie installiert werden. Beide Enden des Bussegments müssen mit einem Widerstandsnetzwerk, wie in Abbildung 1 gezeigt, abgeschlossen werden.

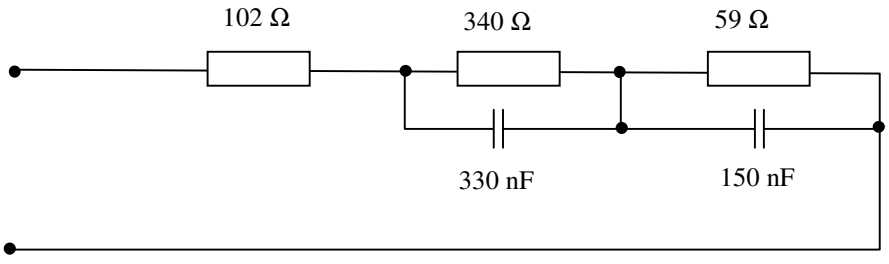

Abbildung 1: TP/XF-1250 Terminierung

3.2.2 TP/FT-10

TP/FT-10 Netzwerkanschlüsse können auch an Link Power Kanäle (LP-10) angeschlossen werden. Bei freier Topologie ist ein einziges Terminierungsglied (Abbildung 2) zu verwenden. Dabei kann dieses Element an jedem beliebigen Ort im Netzwerksegment angebracht werden.

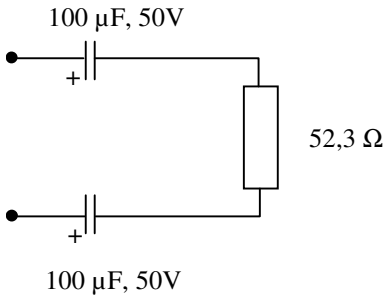

Abbildung 2: TP/FT-10 Terminierung bei freier Topologie

Bei Verwendung einer FT-10 Bustopologie müssen beide Leitungsenden mit einem Terminierungsglied nach Abbildung 3 abgeschlossen werden.

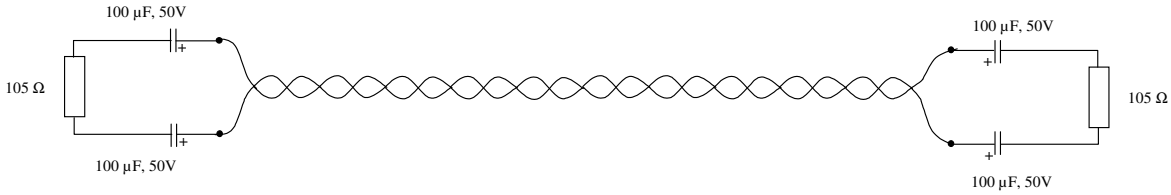

Abbildung 3: Terminierung eines TP/FT-10 Segments in Bustopologie

3.3 Kanalauslastung

Tabelle 2 zeigt die maximal mögliche Paketrate auf ausgewählten Kanälen. Um Kollisionen auf dem Kanal zu vermeiden, soll die tatsächliche Datenrate nicht höher als ca. 70% der maximalen Datenrate betragen.

Kanaltyp	maximale Datenpakete/s (ca.)
TP/FT-10	200-250
TP/XF-1250	600-800

Tabelle 2: Maximale Paketrate auf ausgewählten Kanälen

4 Netzwerkaufbau

4.1 Globale und lokale Kanäle

In Gebäudenetzwerken kann der Datenverkehr in zwei Gruppen aufgeteilt werden:

1. Lokaler Datenverkehr. Dieser beschreibt jene Nachrichten, die zwischen den Knoten in einem lokal eingeschränkten Bereich, wie beispielsweise einem Büroraum, einer Büroetage oder einer Technikzentrale, ausgetauscht werden. Schaltkommandos für die Beleuchtung oder die Sollwertvorgabe und Regelung von Raumtemperaturen über lokale Bediengeräte oder Automationsstationen fallen in den Bereich des lokalen Datenverkehrs.

2. Globaler Datenverkehr. Dieser beschreibt die Daten, die von Knoten in der Feldebene mit übergeordneten Knoten ausgetauscht werden. Beispiele für globalen Datenverkehr sind die Kommunikation mit einer Gebäudeleittechnik, Managementkommandos für die Wartung und Inbetriebnahme sowie globale Informationen von einer Wetterstation, die an mehrere Knoten im Netz verteilt werden.

Dieser Datenverkehr spiegelt sich auch in der zu verwendenden Netzwerkinfrastruktur wider. Kleine Netzwerksegmente, auf denen die Knoten der Feldebene angeschlossen werden, werden mit Hilfe von Netzwerkinfrastrukturkomponenten an einen Hochgeschwindigkeitskanal (Backbone) angebunden, der heute in der Regel als IP-852 (Ethernet/IP) ausgeführt wird. Die Netzwerkinfrastrukturkomponenten sorgen dafür, dass der lokale Datenverkehr auf den lokalen Kanälen verbleibt, der globale Datenverkehr von den übergeordneten Knoten jedoch zuverlässig zu den lokalen Zielknoten gelangt. Abbildung 4 zeigt eine solche Netzwerkstruktur.

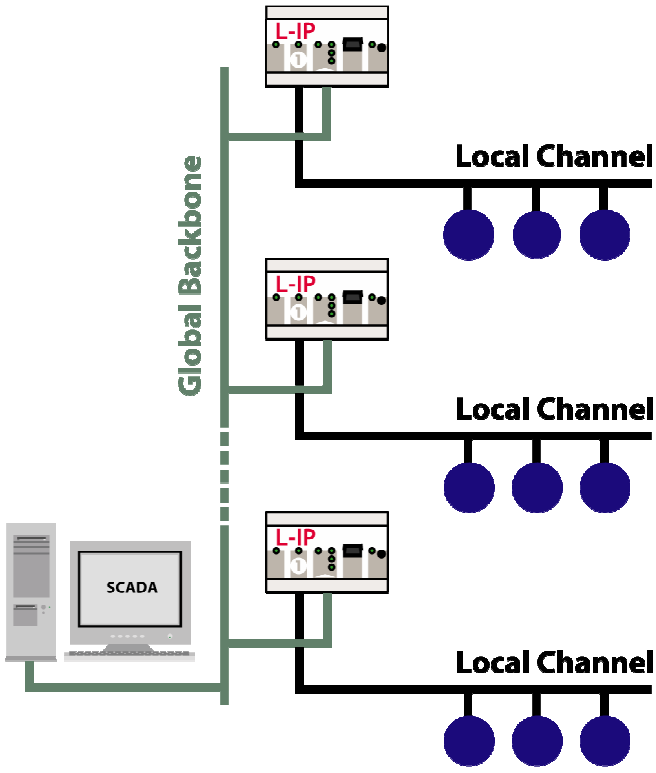

Abbildung 4: Lokale Kanäle, verbunden über einen globalen Backbone-Kanal

Der Transceivertyp der lokalen Geräte muss entsprechend den anzuschließenden Feldgeräten gewählt werden. Dabei wird meist ein TP/FT-10 Kanal eingesetzt. Der Kanaltyp für den Backbone-Kanal kann neben einem IP-852 Kanal je nach benötigter Bandbreite und gemäß den Anforderungen an Kabellängen und Knotenanzahl auch als TP/XF-1250 oder TP/FT-10 Kanal ausgeführt werden.

4.2 Backbone-Kanäle mit geringem Datenaufkommen

In Netzwerken mit wenig Datenverkehr auf dem Backbone-Kanal kann die auf einem TP/FT-10 Kanal verfügbare Bandbreite (78 kbit/s) ausreichend sein. Das Beispiel in Abbildung 5 zeigt ein Netzwerk, das einen TP/FT-10 Kanal als Backbone-Kanal verwendet. Verschiedene L-Switch Router verbinden die lokalen Kanäle mit dem Backbone. Die L-Switch Router können je nach Anzahl der lokalen Kanäle, die in einem Subsystem (beispielsweise ein einzelnes Stockwerk in einem Bürogebäude) benötigt werden, gewählt werden.

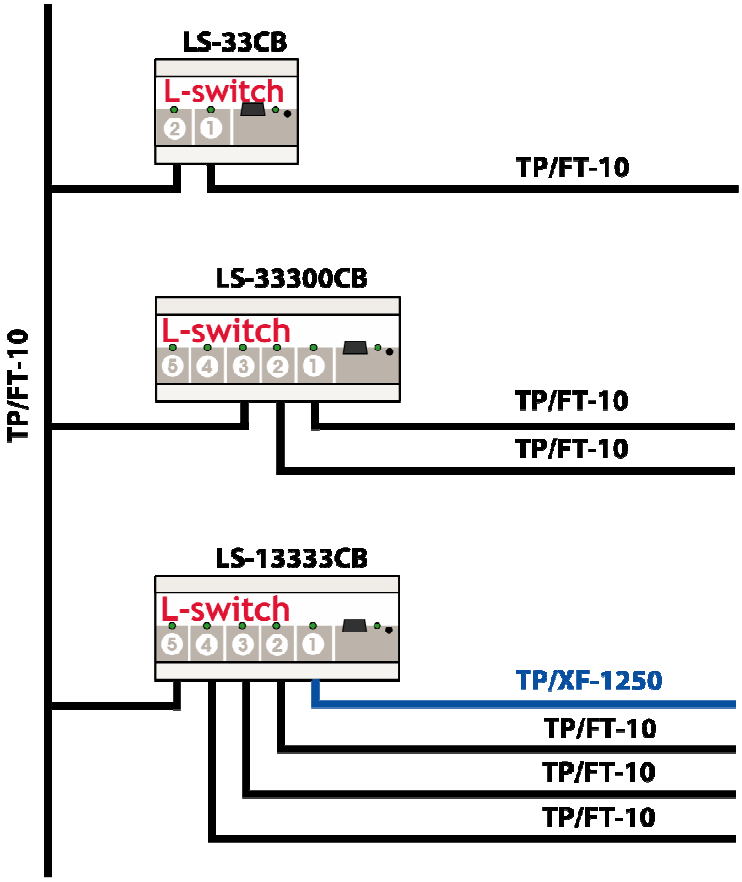

Abbildung 5: Netzwerk mit TP/FT-10 Backbone-Kanal

4.3 Backbone mit TP/XF-1250 Kanal

Meist wird für den Backbone ein höherer Datendurchsatz als für die lokalen Kanäle gefordert. Der TP/XF-1250 Kanal bietet (mit 1,25 Mbit/s) eine Bandbreite, um diese Anforderung in vielen Fällen zu erfüllen. Abbildung 5 zeigt ein Netzwerk mit einem TP/XF-1250 Backbone-Kanal. Die L-Switch Router vom Typ LS-1xxxxCB verbinden eine Klemme mit dem Hochgeschwindigkeits-Backbone und einen oder mehrere TP/FT-10 Kanäle für die lokalen Feldsegmente.

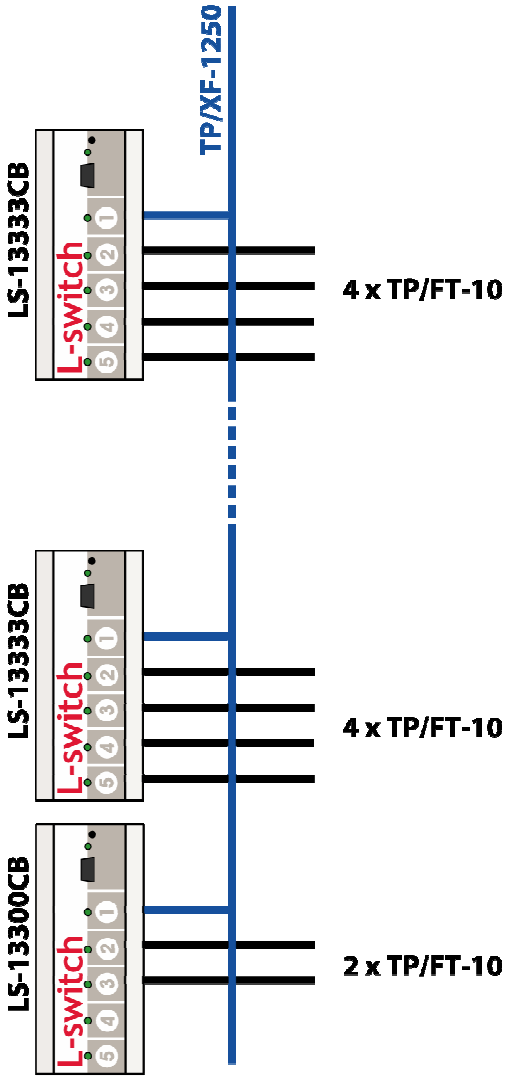

Abbildung 6: Netzwerk mit TP/XF-1250 Backbone-Kanal

Wenn der Backbone-Kanal auf Grund von erhöhten Anforderungen an die Kabellänge verlängert werden muss, so kann eine Struktur entsprechend Abbildung 7 gewählt werden.

Hinweis: Es wird empfohlen, den Backbone-Kanal nicht öfter als 5 mal zu verlängern.

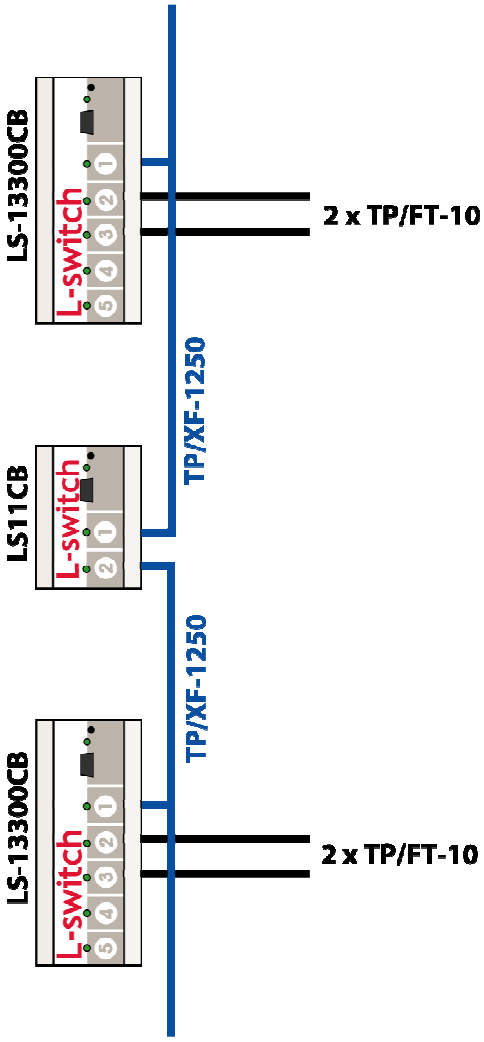

Abbildung 7: Netzwerk mit TP/XF-1250 Backbone-Kanal. Der Backbone wird mit Hilfe eines LS-11C verlängert.

4.4 IP-852 Backbone Kanal

Immer mehr setzt sich die Verwendung von Ethernet/IP als Übertragungsmedium für einen IP-852 Backbone-Kanal durch. Als zukunftssichere Kommunikationstechnologie bietet Ethernet/IP neben einer äußerst hohen Übertragungsrate auch einen flexiblen Zugriff von zentraler Stelle aus auf das gesamte Netzwerk. Beim Einsatz der entsprechenden IP-Netzwerkinfrastruktur ist die Kommunikation sowohl über ein Intranet als auch über das Internet möglich.

Zum Aufbau eines IP-852 Kanals wird ein Konfigurationsserver (Configuration Server) benötigt. Sämtliche L-IP Router haben bereits einen Configuration Server eingebaut. Der Server wird bei genau einem (beliebigen) L-IP Router pro IP-852 Kanal aktiviert. Die IP Adressen aller Kanalteilnehmer werden in die Liste der Kanalteilnehmer (Channel Member List) im Configuration Server eingetragen. Der Configuration Server (CS) verwaltet die Abbildung zwischen Domain/Subnet/Node/Gruppen-Adressen und IP Adressen. Bei Änderungen der Netzwerkkonfiguration senden die Kanalteilnehmer die neue Information zum Configuration Server (blaue Pfeile in Abbildung 8). Dieser verteilt die Information an die übrigen Kanalteilnehmer (rote Pfeile in Abbildung 8). Ein L-IP Configuration Server kann bis zu 256 Kanalteilnehmer verwalten, wobei sich die Kanalteilnehmer auch in unterschiedlichen Domains befinden können.

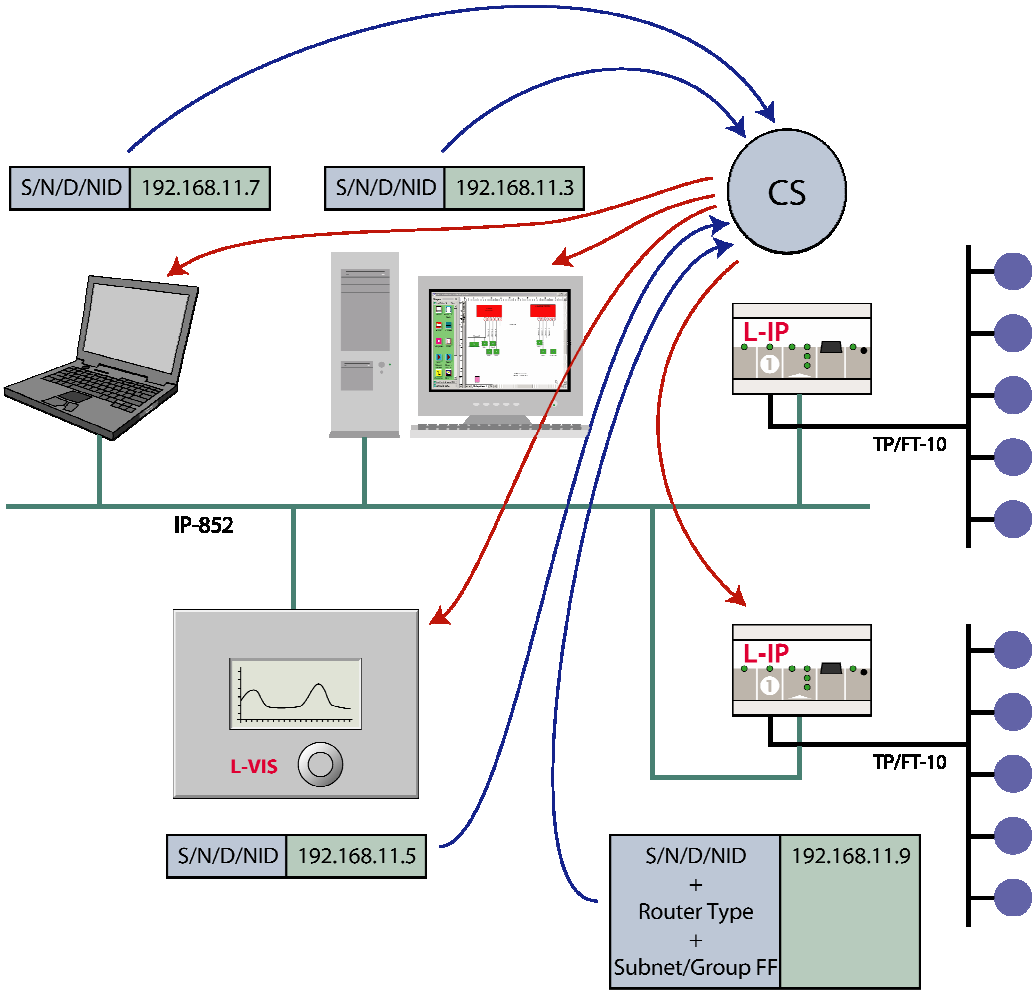

Abbildung 8: Configuration Server für IP-852 Kanäle

In Netzwerken, in denen ein hoher Datendurchsatz zusammen mit einer flexiblen Netzwerkstruktur sowie Ferndiagnose und –wartung benötigt wird, stellt der IP-852 Kanal für den Backbone die optimale Lösung dar (Abbildung 9). Zum Beispiel können TP/FT-10 Kanäle über den IP-852 Backbone-Kanal mit Hilfe von L-IP Routern verbunden werden.

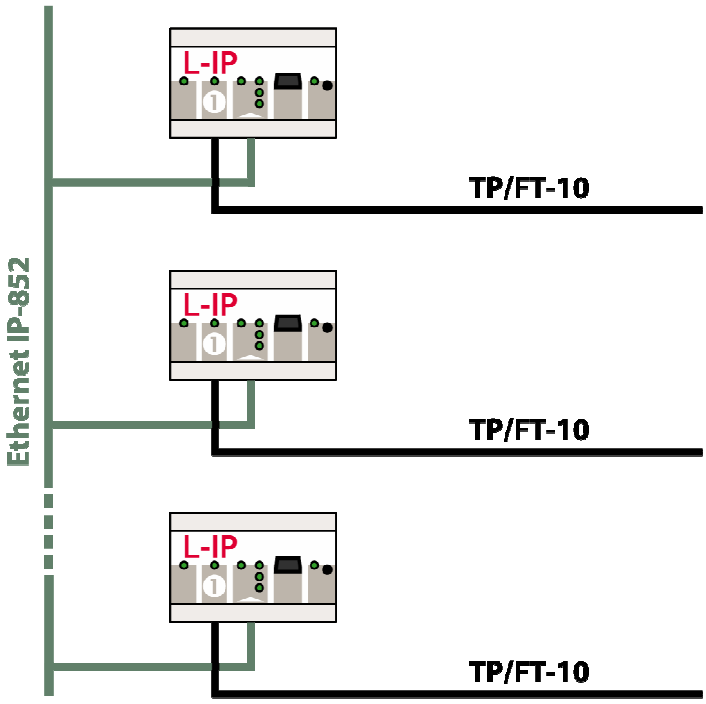

Abbildung 9: IP-852 Backbone mit lokalen TP/FT-10 Kanälen

Zur Anbindung von mehr als einem TP/FT-10 Kanal an einen IP-852 Backbone Kanal können Multiport L-IPs (Abbildung 10) eingesetzt werden.

Ein Vorteil von IP-852 Backbone Kanälen ist, dass die bereits vorhandene Ethernet Netzwerkinfrastruktur weiterverwendet werden kann, was Kosten bei der Erweiterung oder Umrüstung von bereits bestehenden Netzwerken sparen kann. Außerdem ist es möglich, mit Hilfe von IP-852 Kanälen Backbones zu bilden, die sich über mehrere Gebäude oder sogar über voneinander weit entfernt liegende Standorte erstrecken. Wenn das Gebäudemanagementsystem am Backbone angeschlossen wird, so können auch mehrere Standorte einfach in ein einziges System integriert werden (Abbildung 11).

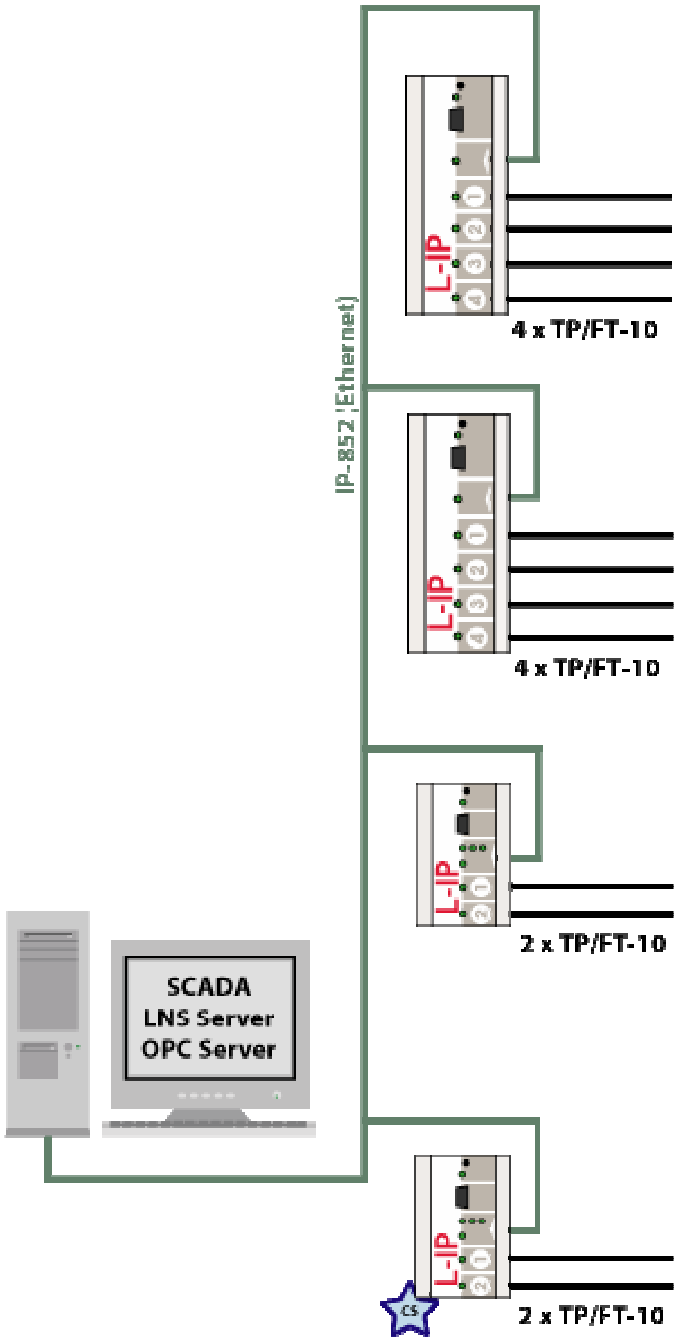

Abbildung 10: Verbinden von mehreren FT-10 Kanälen über Multiport L-IP

Ein weiterer Vorteil eines IP-852 Backbones aus Abbildung 9, Abbildung 10 und Abbildung 11 gegenüber einer Lösung mit TP/XF-1250 Backbone ist, dass die L-IP Router auch als ferngesteuerte Netzwerkschnittstelle zur entfernten Netzwerkanalyse verwendet werden können. Das Kapitel 8 in diesem Dokument enthält weitere Informationen dazu.

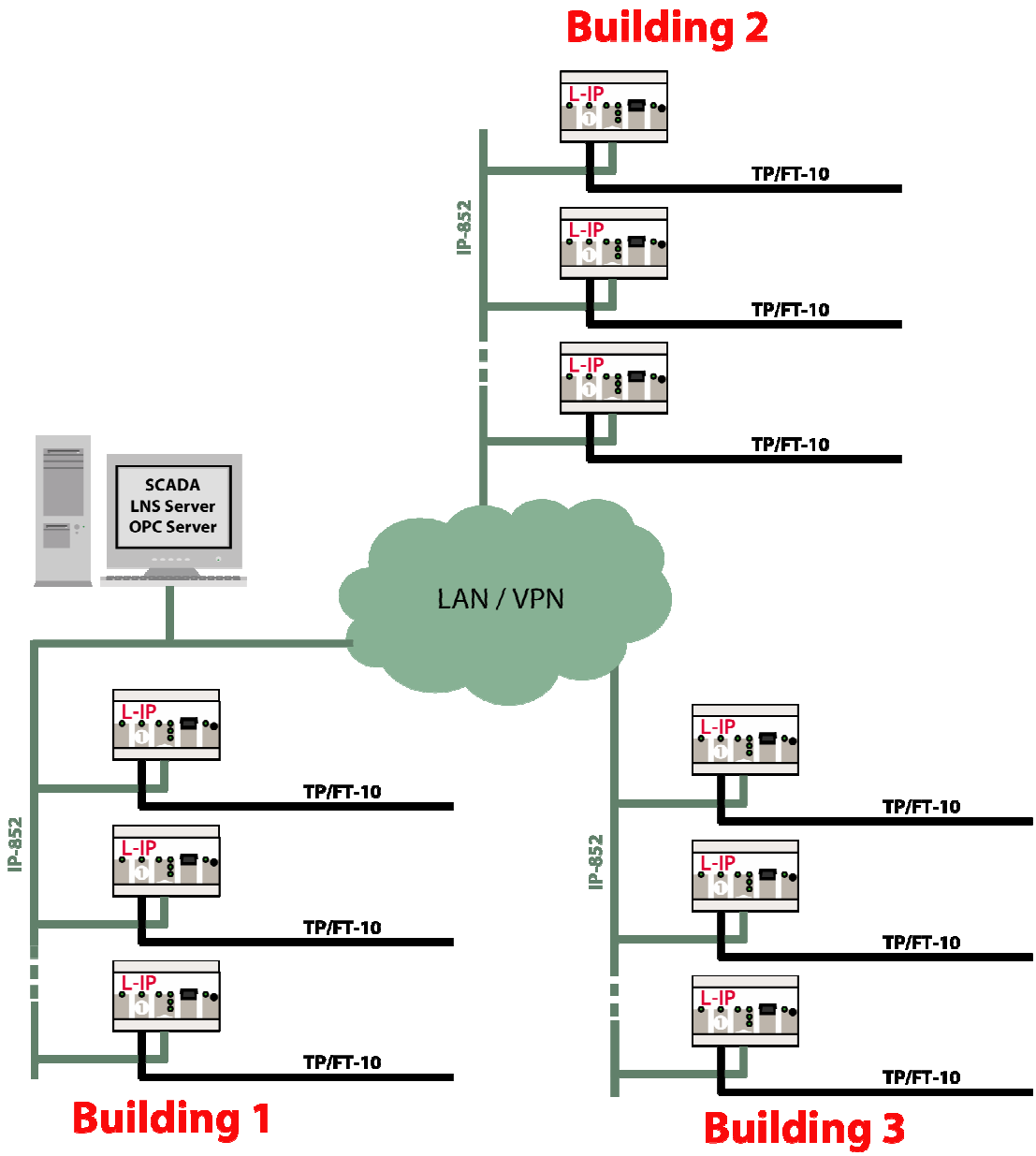

Abbildung 11: Verwendung eines IP-852 Backbones um mehrere Gebäude mit einem einzelnen BMS System zu überwachen.

Mit Blick auf Übertragungsgeschwindigkeit, Flexibilität und Ausfallsicherheit ist eine wie in Abbildung 10 und Abbildung 11 dargestellte flache Netzwerkhierarchie mit IP-852 Kanal als Backbone die optimale Lösung und allen anderen Varianten vorzuziehen.

Eine weitere Möglichkeit ist eine Kombination aus IP-852 Kanälen und TP/XF-1250 Kanälen, um Systeme in mehreren getrennten Gebäuden zu einem einzigen System zusammenzufassen. Dabei kann eine bereits existierende Ethernet-Verbindung genutzt werden, um die Gebäude über einen IP-852 Kanal zusammenzufassen. Innerhalb der einzelnen Gebäude könnten die Backbones mit TP/XF-1250 Kanälen implementiert sein (Abbildung 12). In diesem Beispiel wird ein BMS System für alle Gebäude am TP/XF-1250 Backbone im Gebäude 3 angeschlossen.

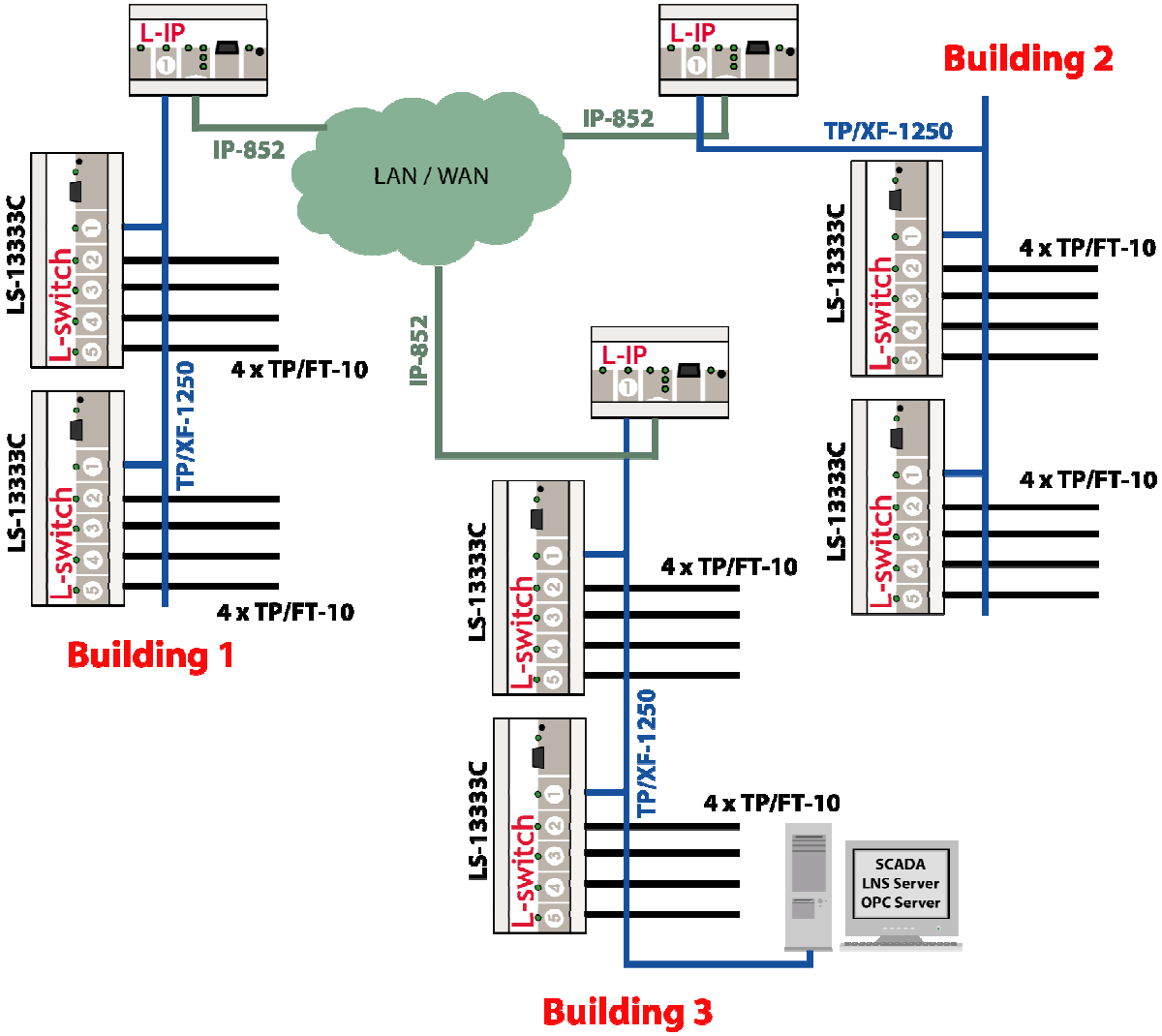

Abbildung 12: Verbinden von mehreren Gebäuden über einen IP-852 Kanal. Innerhalb der Gebäude werden TP/XF-1250 Backbones eingesetzt.

5 Verteilte Netzwerke mit (NAT) Firewalls und dynamischen IP Adressen

Bei Netzwerken, die mehrere Standorte über einen IP-852 Kanal verbinden, kommt es häufig vor, dass die IP Netzwerke durch eine Firewall von der „Außenwelt“ abgeschirmt werden. Zumeist beinhalten die Firewalls auch einen NAT (Network Address Translation) Router der dazu dient, das gesamte Netzwerk hinter dem Router durch eine einzige öffentliche (public) IP Adresse zu repräsentieren. Für die Verwendung von IP-852 Geräten hinter diesen NAT Routern ergeben sich daraus wesentliche Konsequenzen in Bezug auf die Verwendbarkeit der Komponenten und deren Konfiguration. Diese Zusammenhänge sollen in diesem Abschnitt näher erläutert werden. Im Folgenden werden die Begriffe „NAT Firewall“ und „NAT Router“ synonym verwendet.

5.1 Betrieb eines L-IPs hinter einer NAT Firewall

Wie in den vorangegangenen Kapiteln beschrieben, erfolgt der Datenaustausch auf IP-852 Kanälen, indem die Geräte Pakete an die vom Configuration Server mitgeteilten IP Adressen senden. Im Unterschied zu einem lokalen Netzwerk ist jedoch beim Betrieb von Geräten hinter einer NAT Firewall die IP Adresse der Zielgeräte nicht direkt erreichbar. Wie in Abbildung 13 gezeigt, „verstecken“ sich die L-IPs hinter den Firewalls.

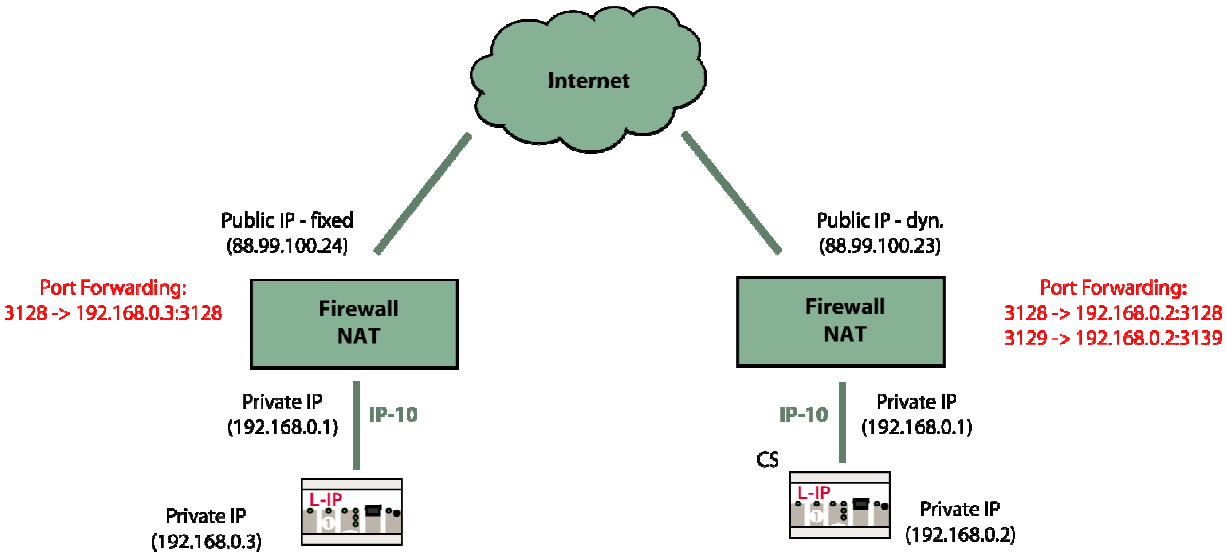

Abbildung 13: Einzelne L-IPs hinter NAT Firewalls

Die NAT Firewall hat zwei Adressen: eine public IP Adresse, über die sie vom öffentlichen Netz aus erreichbar ist, sowie eine private IP Adresse, auf der sie vom lokalen Netz aus angesprochen werden kann. In der Regel ist diese lokale Adresse als Standard-Gatewayadresse in den Geräten im lokalen Netzwerk eingetragen. Um einen L-IP hinter der Firewall zu erreichen, muss ein Knoten auf einem IP-852 Kanal daher zunächst das Paket an die nach außen sichtbare Public-Adresse der Firewall senden. In der Firewall wird eine Port Forwarding-Regel definiert, die festlegt, an welche interne Adresse ein extern auf einem bestimmten Port empfangenes Paket weitergeleitet wird. Will beispielsweise der linke L-IP in

Abbildung 13 ein Paket an den rechten L-IP senden, so muss das Paket an die public IP Adresse der rechten Firewall (88.99.100.23) an den Port 3128 gesendet werden. Die rechte Firewall entscheidet dann auf Grund der zuvor definierten Port Forwarding Regel, dass dieses Paket an den L-IP (192.168.0.2, Port 3128) weitergeleitet werden soll. Für den Server-Port des Configuration Servers wird auf die gleiche Weise eine Port Forwarding Regel definiert.

Im Configuration Server (CS) muss dann zusammen mit der IP Adresse und Clientportnummer des L-IP auch die public IP Adresse der NAT Firewall, hinter der der L-IP angeschlossen wurde, als „NAT-Adresse" konfiguriert werden. Details zu den Einstellungen des L-IP Configuration Servers finden Sie in [6].

5.2 Betrieb mehrerer L-IPs hinter einer NAT Firewall

Werden hinter einer NAT Firewall mehrere L-IPs betrieben, so müssen die L-IPs auf unterschiedlichen Client-Ports eingestellt werden. In der NAT Firewall werden dann die entsprechenden Port-Forwarding Regeln definiert (siehe Abbildung 14). In dem beschriebenen Beispiel werden alle Pakete, die die rechte NAT Firewall auf port 3128 ihrer public Adresse empfängt, intern an die IP Adresse 192.168.0.2, Port 3128 weitergeleitet. Die Pakete auf Port 3130 gehen an die interne IP Adresse 192.168.0.3, Port 3130.

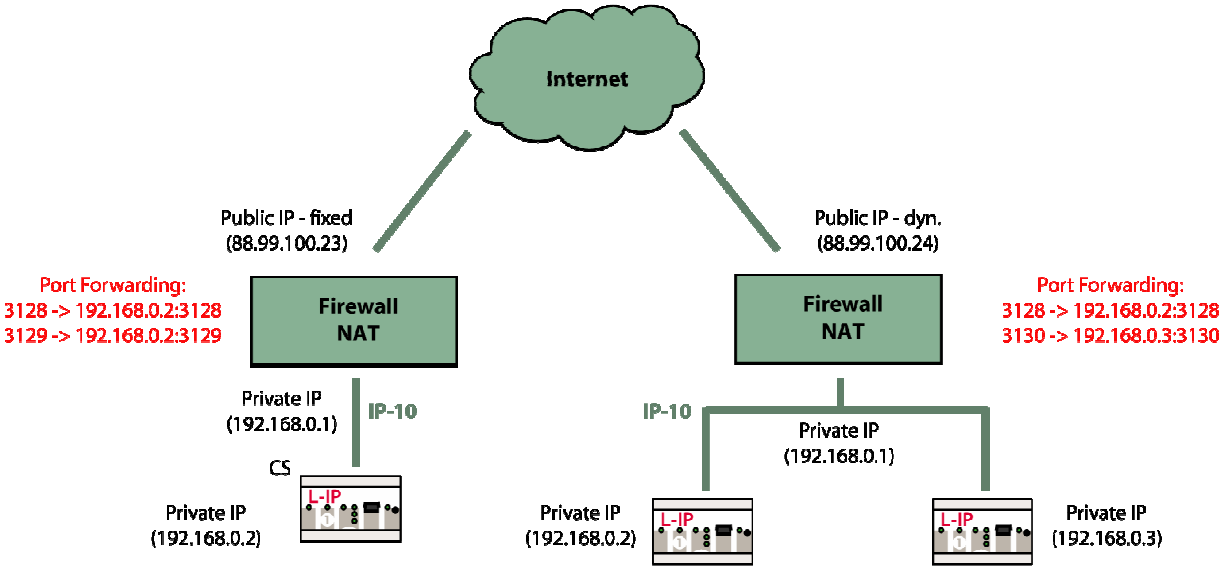

Abbildung 14: Betrieb mehrerer L-IPs hinter einer NAT Firewall

Befinden sich mindestens 2 Geräte hinter einer NAT Firewall in einem IP-852 Kanal, so wechselt der Configuration Server in den „Extended NAT" Modus. In dieser Konfiguration können Pakete mit anderen L-IPs und LOYTEC Produkten, nicht jedoch mit IP-852 Routern anderer Hersteller ausgetauscht werden.

5.3 Betrieb eines PCs hinter einer NAT Firewall

Es ist auch möglich, einen IP-852 Kanal mit einem hinter einer NAT Firewall befindlichen PC zu betreiben. Dazu wird als Netzwerkinterface für den PC ein NIC-852 benötigt (siehe Abbildung 15). In der Konfigurationssoftware für den NIC-852 muss dabei neben der Adresse für den Configuration Server auch die public IP Adresse des NAT Routers, hinter dem sich der PC befindet, eingetragen werden (im Beispiel 88.99.100.22). Die Port-Forwarding Regeln müssen im NAT Router äquivalent zu den Einstellungen beim Betrieb eines L-IPs hinter der Firewall eingetragen werden.

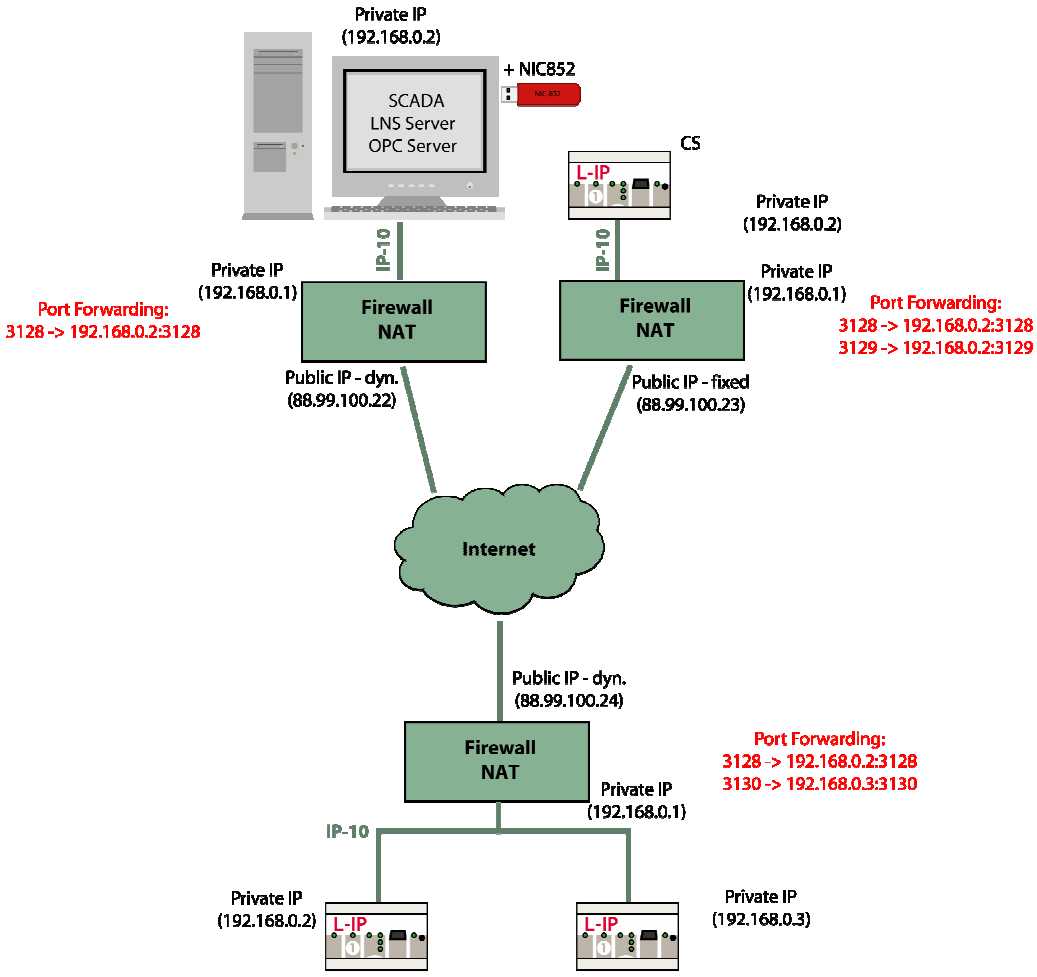

Abbildung 15: PC mit NIC-852 hinter einer Firewall

5.4 Einstellungen für den Betrieb mit dynamischen IP Adressen

Innerhalb eines Gebäudenetzwerks werden den Geräten am IP-852 Kanal (L-IP, PC, L-Vis,…) zumeist fixe IP Adressen zugewiesen, da diese ja fix in des Gebäude integriert sind und sich ihr Standort nicht dynamisch verändert. Bei Betrieb von NAT Firewalls ist es jedoch oft der Fall, dass die öffentliche (public) IP Adresse dem NAT Router dynamisch zugewiesen wird. Dadurch kann es passieren, dass sich die Adressen während des Betriebs ändern. Diese Adressänderung muss auch im Configuration Server nachgezogen werden. Der Configuration Server verteilt dann die geänderten Adressen an die anderen Kanalteilnehmer am IP-852

Kanal. Aus nahe liegenden Gründen ist ein manuelles Nachziehen der Adressen in der Praxis nicht möglich. Daher bietet der L-IP Configuration Server mit der „Roaming Member“ Option die Möglichkeit, automatisch veränderte IP Adressen zu erkennen und diese in der Channel Member List nachzuführen sowie die Informationen an alle Kanalteilnehmer weiterzuleiten. Es können ein oder mehrere Geräte im Kanal hinter NAT Routern mit dynamischen IP Adressen betreiben werden. Die einzige Einschränkung bezieht sich auf die IP Adresse des NAT Routers, hinter dem sich der L-IP mit aktivierten Configuration Server befindet: diese IP Adresse muss fix sein, da die anderen Geräte ansonsten den Configuration Server bei einer Adressänderung nicht mehr kontaktieren können.

6 Smart Switch Modus und Configured Router Modus

Die L-Switch^{XP} Router und L-IP Router können in zwei Betriebsmodi verwendet werden. Im Smart Switch Modus lernt das Gerät selbständig die Netzwerktopologie auf Grund der in den Datenpaketen enthaltenen Absenderadressen. Im Configured Router Modus muss das Netzwerk Management Programm die Routing-Tabellen entsprechend der Netzwerkkonfiguration in die Geräte schreiben. Änderungen an der Netzwerkstruktur erfordern daher im Configured Router Modus immer auch eine Veränderung der Routing-Tabellen durch das Netzwerk Management Programm. Tabelle 3 zeigt, welcher Modus in welchem Gerät ausgewählt werden kann sowie den eingestellten Betriebsmodus im Auslieferungszustand.

Gerät	Smart Switch Modus	Router Modus
L-Switch Router	Ja (Auslieferungszustand)	Nein
L-Switch^{XP} Router	Ja (Auslieferungszustand)	Ja
L-IP Router	Ja	Ja (Auslieferungszustand)

Tabelle 3: Betriebsmodi und Grundeinstellungen.

6.1 Smart Switch Modus

Im Smart Switch Modus lernen LOYTEC Router die Netzwerkstruktur anhand der empfangenen Datenpakete und leiten die Datenpakete entsprechend der bereits gelernten Information an die angeschlossenen Netzwerksegmente weiter. Der Lernalgorithmus basiert darauf, dass die Adressen immer

- aufgrund der **Absenderadresse gelernt** und
- aufgrund der **Zieladresse weitergeleitet** werden.

Datenpakete, die an noch nicht bekannte Zieladressen gesendet werden sollen, werden an alle Netzwerkanschlüsse (mit Ausnahme des Netzwerkanschlusses, auf dem das Datenpaket empfangen wurde) weitergeleitet. Der Lernalgorithmus kann sowohl Subnet/Node Adressen als auch Gruppenadressen lernen. Da die Netzwerkstruktur immer aufgrund der Absenderadresse gelernt wird, können Subnet/Node Adressen nur von Knoten gelernt werden, die selbst aktiv Datenpakete aussenden. Datenpakete zu Knoten, die ausschließlich Datenpakete empfangen und selbst keine Datenpakete aussenden, werden daher immer auf alle Netzwerkanschlüsse der Infrastrukturgeräte weitergeleitet. Für den Lernalgorithmus sind bereits die Acknowledgement-Datenpakete ausreichend, um die Subnet/Node Adresse eines

Knoten zu lernen. Das bedeutet, dass, sofern eine Kommunikation zwischen zwei Knoten im acknowledged Übertragungsdienst stattfindet, bereits die Subnet/Node Adressen von beiden Knoten gelernt werden können. Da während der Inbetriebnahme mit einem Installationstool eine Reihe von Datenpaketen zwischen dem Installationsprogramm und jedem einzelnen Knoten ausgetauscht werden, wir in den meisten Fällen die Netzwerkstruktur bereits während der Inbetriebnahme des Netzwerks gelernt.

Um Gruppenadressen zu lernen, muss zumindest eine Nachricht innerhalb der Gruppe im acknowledged Übertragungsdienst versendet werden. Erfolgt die Kommunikation innerhalb einer Gruppe ausschließlich im ‚Unacknowledged' oder ‚Unacknowledged Repeated' Übertragungsdienst, so werden die Nachrichten, die an diese Gruppe adressiert sind, an alle Netzwerkanschlüsse weitergeleitet.

Um das Gerät im Smart Switch Modus zu betreiben, **darf das Gerät im Netzwerkmanagementprogramm nicht kommissioniert werden**. Es ist jedoch möglich, das Gerät zu Dokumentationszwecken oder um die Kommunikation über verschiedenartige Übertragungskanäle hinweg zu ermöglichen, als „Dummy"-Router in das Netzwerkmanagementprojekt einzufügen. Nähere Informationen dazu können in [3] nachgelesen werden.

Im Smart Switch Modus werden keine Netzwerktopologien mit „Loops" unterstützt. Das bedeutet, dass die Verbindung zweier Knoten im Netzwerk immer nur über genau einen Pfad möglich ist.

6.2 Router Modus

Im Router Modus verhält sich das Gerät wie ein Configured Router. Die Routing-Tabellen werden mit Hilfe des Netzwerkmanagementprogramms geschrieben. Um dies zu er möglichen, **muss das Gerät im Netzwerkmanagementprojekt kommissioniert werden**. Nur der Betriebsmodus „Configured Router" ist für L-Switch^{XP} Router und L-IP Router zulässig. Die Geräte liefern eine Fehlermeldung wenn versucht wird, sie in den Modus „Repeater" oder „Learning Router" zu setzen und zu kommissionieren.

6.3 Empfehlungen zur Verwendung von Smart Switch und Configured Router Modus

Bei der Verwendung von LNS^{TM} basierten Installationstools wird prinzipiell die Verwendung des „Configured Router" Modus empfohlen. Dadurch wird es dem Installationstool erleichtert, Fehler bei der Installation, wie z.B das Anschliessen eines Knoten an einen falschen Kanal, zu erkennen. Der L-IP Router sollte vorzugsweise im "Configured Router" Modus Betrieben werden, da in diesem Modus die Ressourcen des Ethernetkanals effizienter genutzt werden können.

Der Smart Switch Modus ist immer dann ermpfehlenswert, wenn Router nachträglich eingebaut werden und dabei die Netzwerkstruktur im Netzwerkmanagement Tool nicht verändert werden soll. Dieser Modus ist auch hilfreich, wenn das Installationsprogramm die Routingtabellen der Router nicht automatisch richtig setzen kann.

Im Allgemeinen sollte der Configured Router Modus immer auch dann verwendet werden, wenn sich im Netzwerk mehrere Gruppen befinden, die über den ’Unacknowledged’ oder ’Unacknowledged Repeated’ Übertragungsdienstes kommunizieren. Auch in Netzwerken, die Subnet-weite Broadcast-Nachrichten einsetzen, sollte der Configured Router Modus benutzt werden.

7 Multi-Domain Installationen

In einem ANSI/EIA-709 Netzwerk können einzelne Knoten nur mit Knoten in der selben Domain kommunizieren. In LNS basierten Netzwerkmanagement-Programmen entspricht jedes LNS Projekt einer eigenen Domain. Für die meisten Projekte stellt die maximale Anzahl an Knoten, die pro Domain verwendet werden können (32385) keine wesentliche Einschränkung dar. Durch die Beschränkung auf 256 Gruppenadressen pro Domain kann es aber in manchen Projekten notwendig werden, mehrere Domains zu verwenden.

In Projekten mit mehreren Domains (LNS Datenbanken) können L-Proxy Gateways verwendet werden, um Daten über Domaingrenzen hinweg auszutauschen. L-Proxy stellt 5 Ports (2 x TP/FT-10 und 3 x über Ethernet/IP - IP-852) zur Verfügung, von denen jeder netzwerkseitig als unabhängiger Knoten angesprochen werden kann. Jeder Knoten kann somit in einer eigenen Domain eingesetzt werden. Statische, dynamische oder „externe“ (gepollte) Netzwerkvariable, die auf den einzelnen Netzwerkanschlüssen angelegt werden, können mit Hilfe einer Konfigurationssoftware intern verbunden werden. Auf diese Weise wird es möglich, Daten domainübergreifend auszutauschen.

7.1 Verbinden von 2 Domains über FT Kanal

Im einfachsten Fall sollen zwei Netzwerke in unterschiedlichen Domains über FT Kanäle verbunden werden. Dazu kann die Konfiguration in Abbildung 16 verwendet werden.

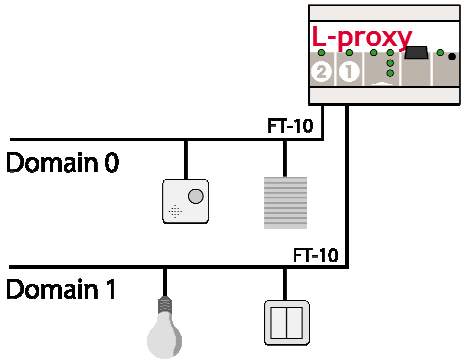

Abbildung 16: L-Proxy Gateway in einem Netzwerk mit 2 Domains.

In dieser Konfiguration werden die IP-852 Ports des L-Proxy nicht benutzt.

7.2 Verwenden von 2 bis 5 Domains

Bis zu 5 Domains können mit einem L-Proxy LP-33E100 verbunden werden. Für die bis zu 5 Domains stehen neben den 2 FT-Ports auch bis zu drei IP Ports auf dem IP-852 Kanal zur Verfügung. Äquivalent zu den FT Ports werden dabei auf dem IP-852 Kanal bis zu 3 Knoten angelegt. Es handelt sich dabei um „virtuelle“ Knoten, die sich alle am selben Ethernet-Kanal befinden, logisch jedoch komplett getrennte Knoten mit eigenständiger Konfiguration darstellen. Zum Betrieb der IP-852 Knoten des L-Proxy muss das Gerät in die Kanalliste

eines Configuration Servers eingetragen werden. Für den gesamten L-Proxy ist nur ein Eintrag erforderlich. Dieser Eintrag repräsentiert die 3 L-Proxy IP-852 Ports.

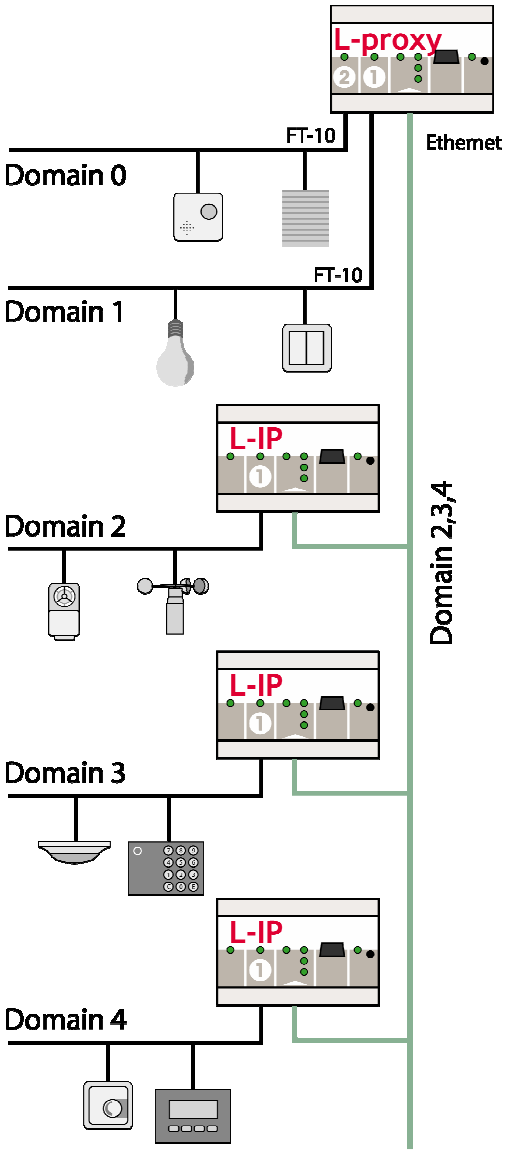

Abbildung 17: Verbinden von bis zu 5 Domains mit einem L-Proxy

Wie in der Abbildung 17 gezeigt, werden die Domains 2,3 und 4 über L-IP Router auf dem IP-852 Kanal zusammengeführt.

7.3 Verbinden von mehr als 5 Domains

Mehr als 5 Domains können durch das Zusammenschalten mehrerer L-Proxy Geräte verbunden werden (siehe Abbildung 18). Ein L-Proxy kann dabei 5 Domains verbinden. Alle weiteren L-Proxy Geräte ergänzen dann weitere 4 Domains, wobei alle L-Proxy Geräte einen der IP-852 Ports in der selben Domain konfiguriert haben (im Beispiel Domain 4), um über diesen Port untereinander Daten auszutauschen.

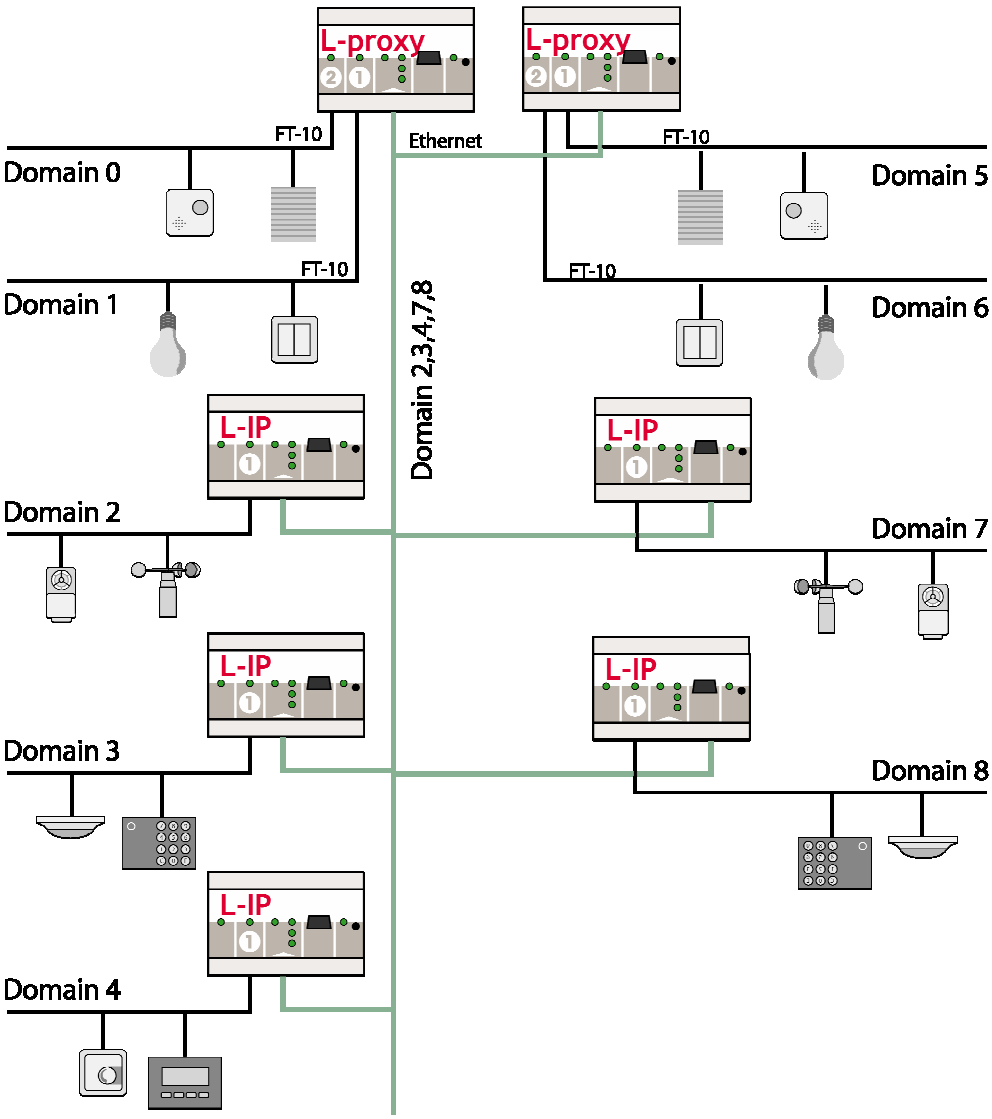

Abbildung 18: 2 L-Proxy zur Verbindung von mehr als 5 Domains

8 Fernwartung und Analyse von Netzwerken

LOYTEC Netzwerkinfrastrukturkomponenten sind mit eingebauten Diagnosefunktionen ausgestattet. Fehler wie Kanalüberlast oder zerstörte Datenpakete werden mit Hilfe von Diagnose-LEDs angezeigt. Blinkt die Port-LED rot, so liegt ein Problem in diesem Netzwerksegment vor (im folgenden als Netzwerküberlastsituation bezeichnet).

Eine Netzwerküberlastsituation tritt auf wenn

- die durchschnittliche Bandbreitenauslastung höher als 70% war.
- mehr als 5% der Nachrichten durch Kollisionen zerstört wurden.
- der Prozentsatz an .Missed Preambles. höher als 5% war.
- mehr als 5% der Nachrichten auf einem Port mit fehlerhaftem CRC empfangen wurden

Die Router zeichnen auch statistische Daten über den Netzwerkverkehr und Fehlerzustände auf. Diese Aufzeichnungen können mit dem LOYTEC Systemdiagnose Programm (LSD Tool) ausgelesen werde. Dieses Programm liefert zahlreiche Informationen um den „Gesundheitszustand“ des Netzwerks beurteilen zu können. Auf LOYTEC Netzwerkinfrastrukturgeräte kann mit dem LSD Tool über lokale Verbindungen vor Ort oder aus der Ferne zugegriffen werden (Abbildung 19). Das LSD Tool findet alle LOYTEC Netzwerkinfrastrukturgeräte über einen lokalen Netzwerkanschluss (1,2), über entfernte IP-852 Verbindungen (3,4) oder über eine NIC709-IP Schnittstelle (5).

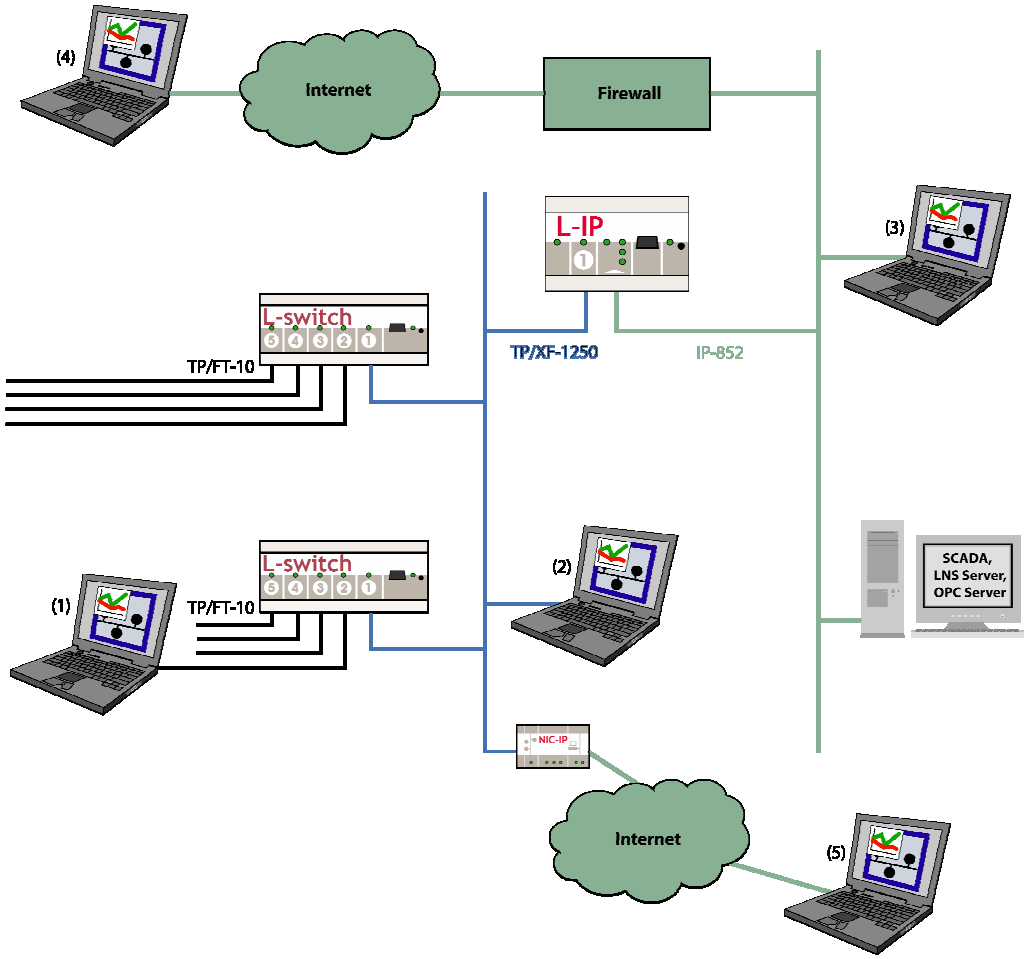

Abbildung 19: Lokaler und entfernter Netzwerkzugriff mit dem LSD Tool.

Zur exakten Analyse von Störungen und Fehlern wird in einem nächsten Schritt der LOYTEC Protokollanalysator LPA verwendet. Der LPA zeichnet die Datenpakete am Netzwerk auf und zeigt sie in einer grafischen Windows Oberfläche an.

Der LPA Protokollanalysator kann jedoch nur jene Datenpakete aufzeichnen, die auf dem Kanal, an dem die Schnittstellenkarte des Analysators angeschlossen ist, übertragen werden. Zur Ferndiagnose von Netzwerken haben die L-IP Router eine Schnittstelle eingebaut, die es der LPA-IP Protokollanalysatorsoftware erlaubt, auf die an den L-IP Router angeschlossenen Kanäle zuzugreifen. So können über ein Ethernet-Netzwerk alle erreichbaren L-IP Router ausgewählt werden und die an die L-IP Router angeschlossenen entfernten Kanäle analysiert werden.

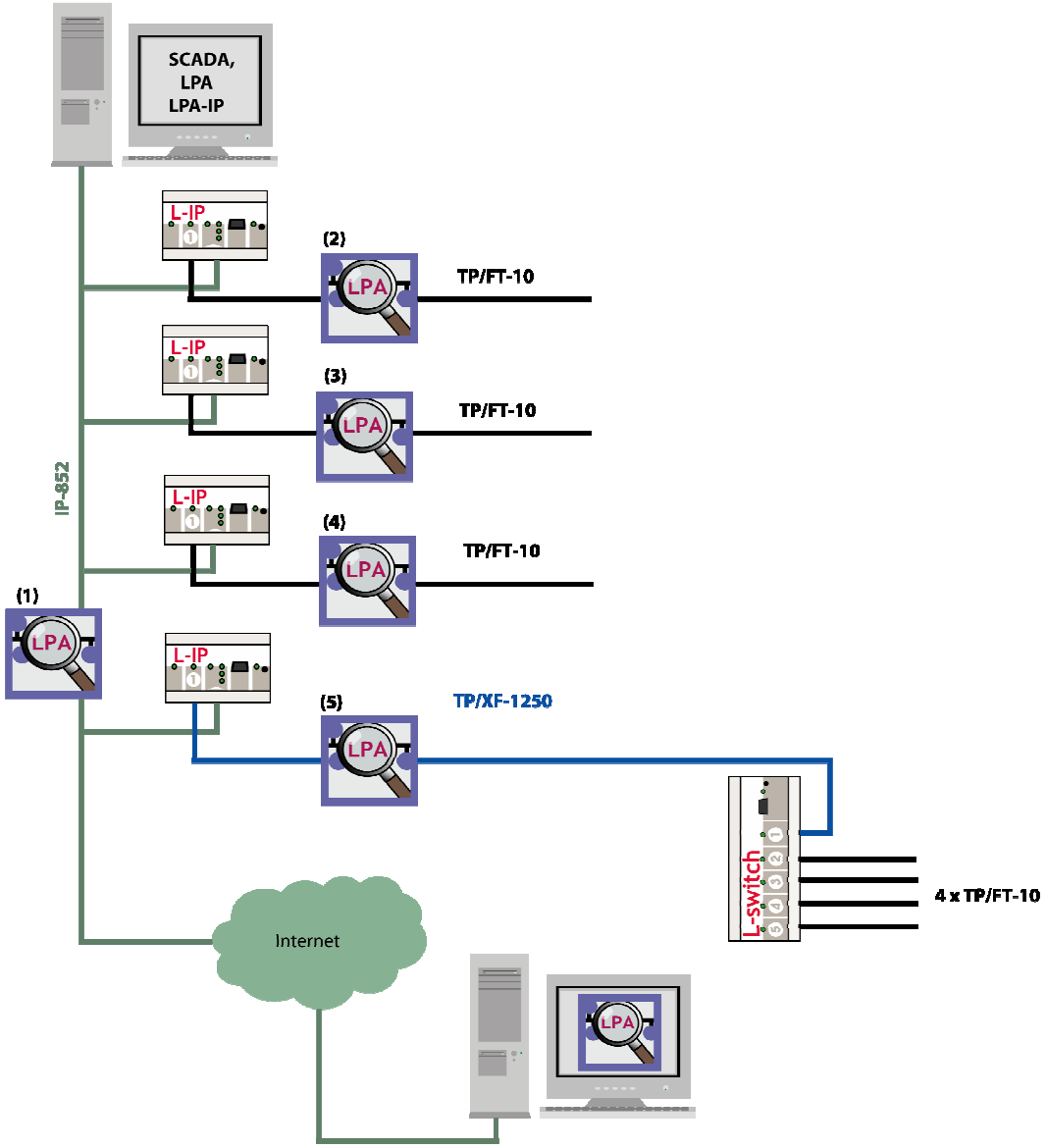

Abbildung 20: Fernanalyse mit dem LPA und LPA-IP.

Abbildung 20 zeigt die unterschiedlichen Möglichkeiten für eine Fernanalyse von Netzwerken. Die LPA-IP Software kann sowohl den Verkehr auf einem IP-852 Kanal (1), als auch den Datenverkehr hinter den L-IP Routern liegender Kanäle aufzeichnen (2,3,4,5).

Netzwerksegmente, die nicht an einen L-IP Router angeschlossen sind, können mit Hilfe einer NIC709-IP Schnittstelle aus der Ferne analysiert werden. Natürlich ist es auch möglich, auf lokalen Kanälen mit Hilfe von verschiedenen Schnittstellenkarten (z. B. NIC709-USB) Analysedaten zu sammeln (Abbildung 21).

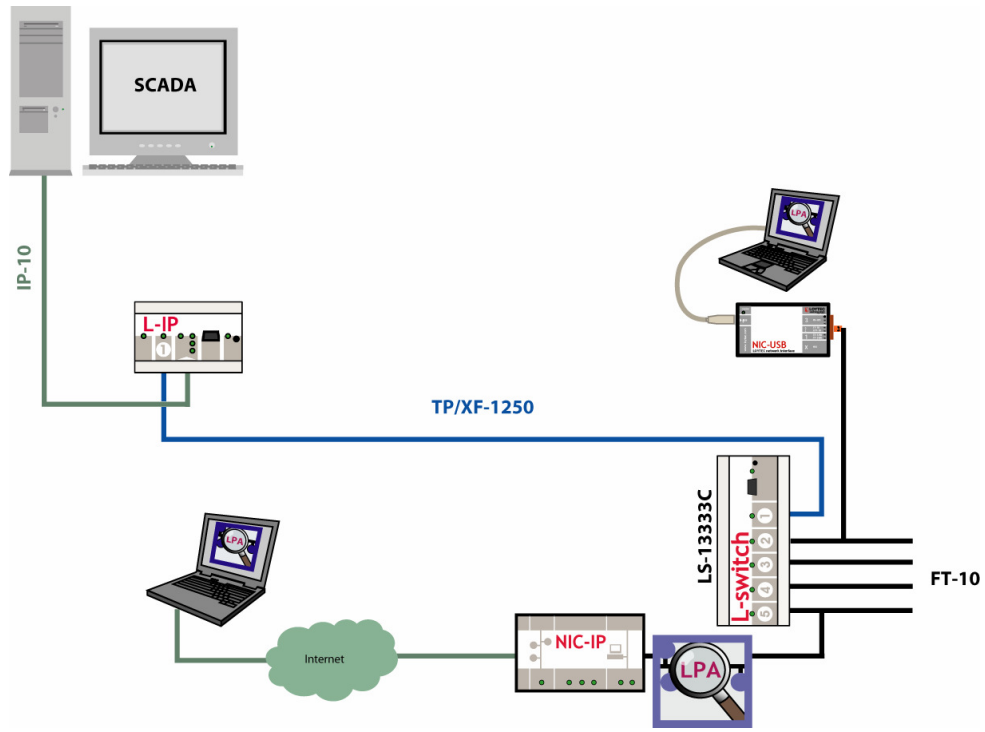

Abbildung 21: Fernzugriff mit Hilfe eines NIC709-IP und lokaler Netzwerkzugriff mit einem NIC709-USB.

9 Fernzugriff über ISDN

In manchen Projekten ist ein Fernzugriff auf ein Netzwerk ohne dauerhafte IP Verbindung gefordert. In solchen Anwendungen kann eine IP Anbindung über einen ISDN Anschluss hergestellt werden. Die Anbindung kann mit Hilfe eines NIC709-IP (siehe Abbildung 22) hergestellt werden. Es kann auch der IP-852 Kanal über die ISDN Verbindung hinweg erweitert werden, wobei der Netzwerkzugriff beispielsweise über einen NIC-852 erfolgt (siehe Abbildung 23). Der zweite Ansatz hat den Vorteil, dass die LPA Fernanalysefunktionalität (siehe Kapitel 7) auch über den ISDN Link hinweg eingesetzt werden kann.

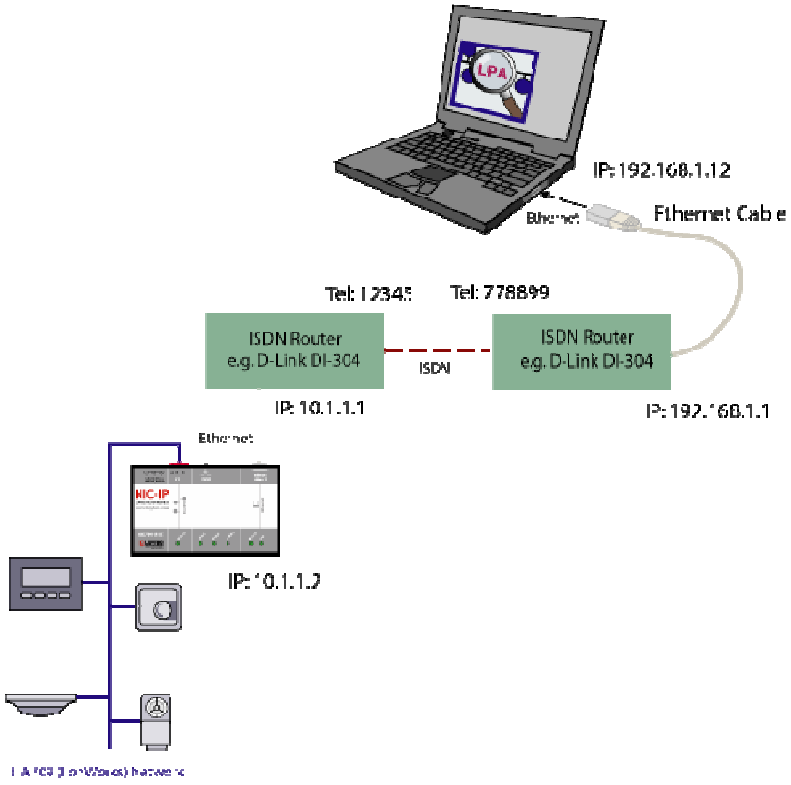

Abbildung 22: Fernzugriff über ISDN mit Hilfe eines NIC709-IP

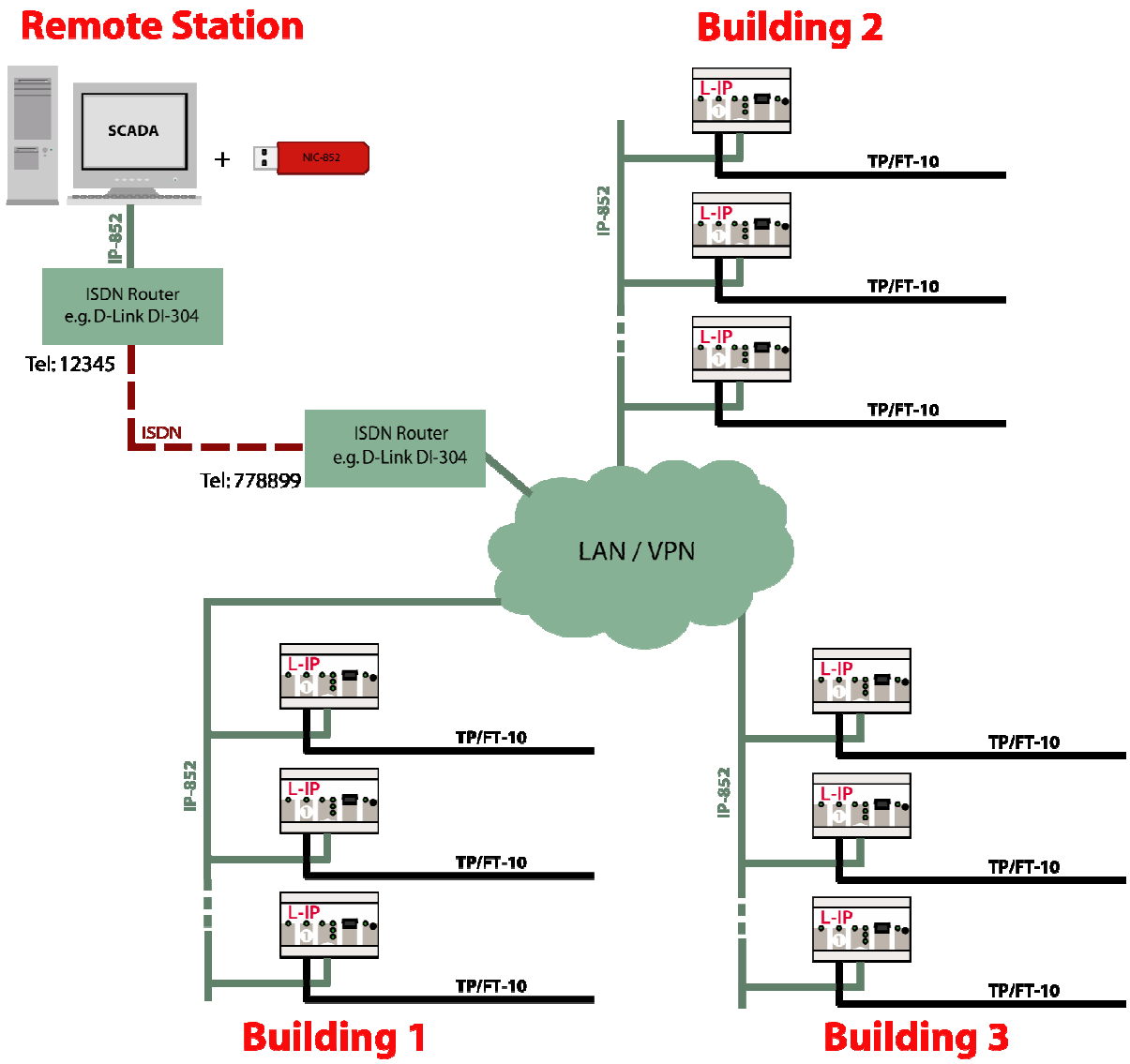

Abbildung 23: Erweiterung eines IP-852 Kanals über eine ISDN Verbindung

Ein ISDN Fernzugang kann auf zwei Arten realisiert werden:

1. Transparente LAN-zu-LAN Verbindung mit Hilfe eines Dial-on-demand Zugangs
2. Einwahlzugang auf einer entfernten Anlage

Einige Computerhardwarehersteller bieten ISDN Geräte mit LAN-zu-LAN und Einwahlunterstützung an. Im Folgenden wird beispielhaft die Konfiguration mit Hilfe eines D-Link DI-304 Routers beschrieben.

9.1 LAN-zu-LAN Verbindung

Die beschriebene Beispielapplikation implementiert die Netzwerkstruktur in Abbildung 22. Der PC ist mit einem der IP Anschlüsse des lokalen ISDN Routers verbunden. Eine direkte Verbindung ist dabei nicht zwingend erforderlich, der lokale ISDN Router muss jedoch über das lokale Netzwerk erreichbar sein und so als Gateway zum NIC-IP verwendet werden können. Der lokale ISDN Router wird so konfiguriert, dass er einen zweiten, entfernten ISDN Router automatisch anwählt und zusammen mit dem zweiten ISDN Router eine transparente IP Verbindung aufbaut. Nach einer vorgegebenen Zeit ohne Netzwerkaktivität wird die Verbindung automatisch wieder abgebaut.

Der D-Link ISDN Router kann über einen eingebauten Webserver konfiguriert werden, wie die folgende Anleitung zeigt:

1. Zunächst müssen die lokalen IP Einstellungen vorgenommen werden (Abbildung 24). In diesem Beispiel wird dem lokalen Router die IP Adresse 192.168.1.1 zugewiesen. Der Router agiert auch als DHCP Server, der IP Adressen beginnend mit Adresse 192.168.1.100 zuweist.

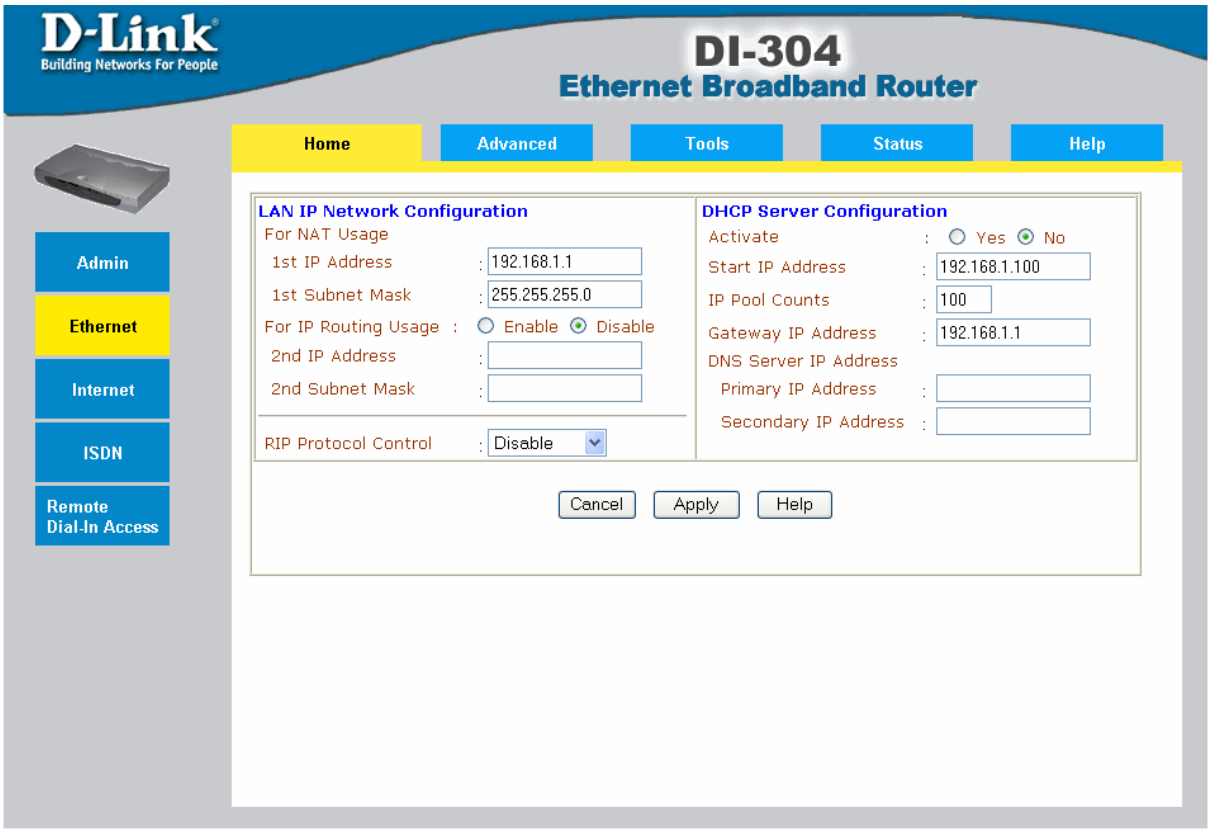

Abbildung 24: Ethernetkonfiguration des lokalen ISDN Routers

2. Danach müssen die ISDN Einstellungen vorgenommen werden (Abbildung 25). Der ISDN Anschluss wird aktiviert und die lokale Telefonnummer eingegeben.

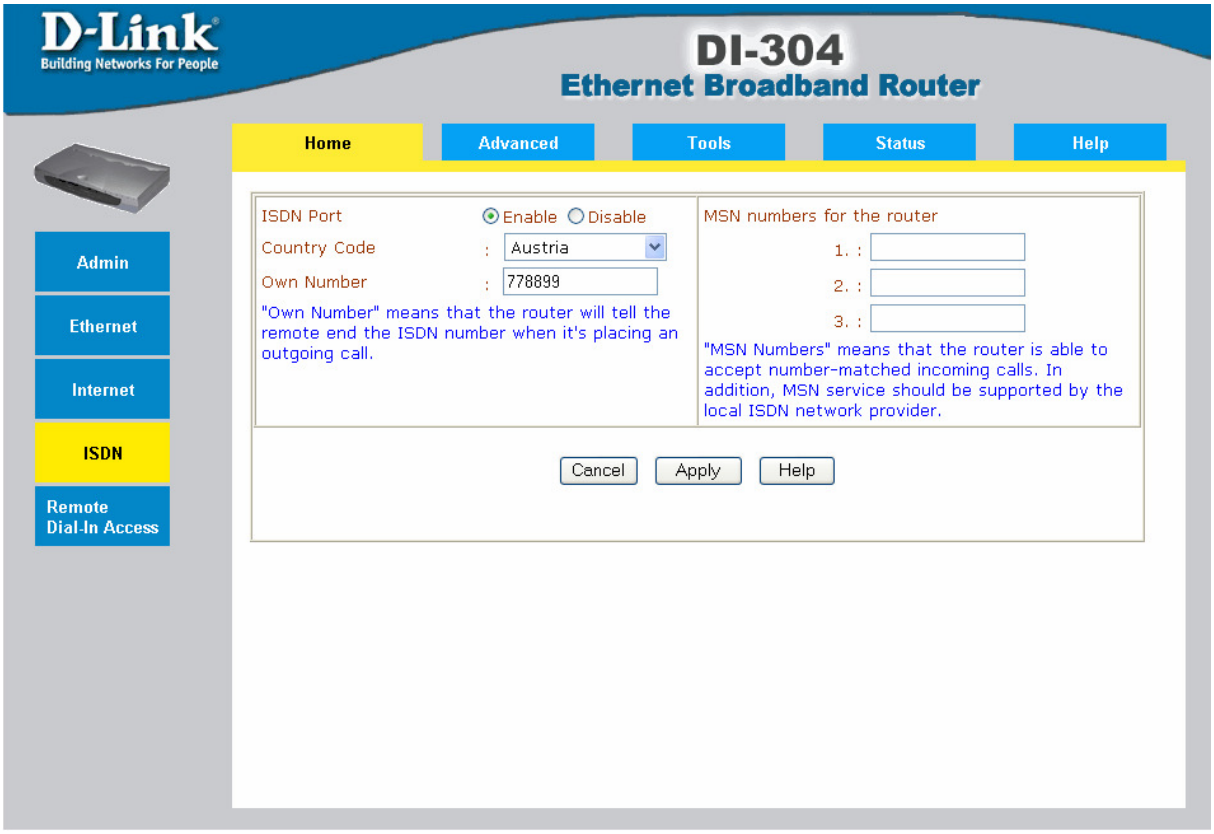

Abbildung 25: ISDN Konfiguration des lokalen Routers

3. Für die automatische Dial-In Funktion muss ein LAN-to-LAN Dialer Profile erstellt werden (Abbildung 26, Abbildung 27, Abbildung 28). Danach wird das Profil aktiviert und die Telefonnummer sowie Benutzername und Passwort des entfernten Routers eingegeben. Für den automatischen Abbau der Verbindung muss noch eine Idle-Zeit eingegeben werden. Optional können weitere Einstellungen wir beispielsweise der ISDN Link-Typ vorgenommen werden.

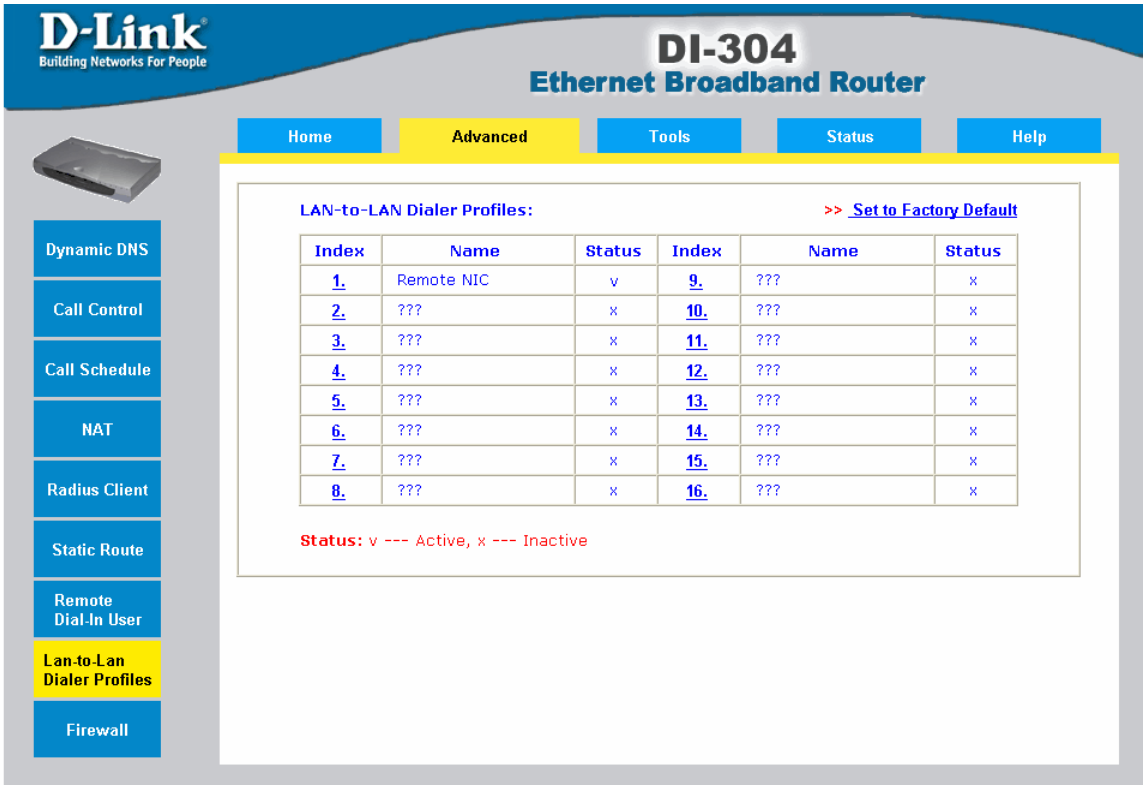

Abbildung 26: Aktivieren der LAN-to-LAN Profile

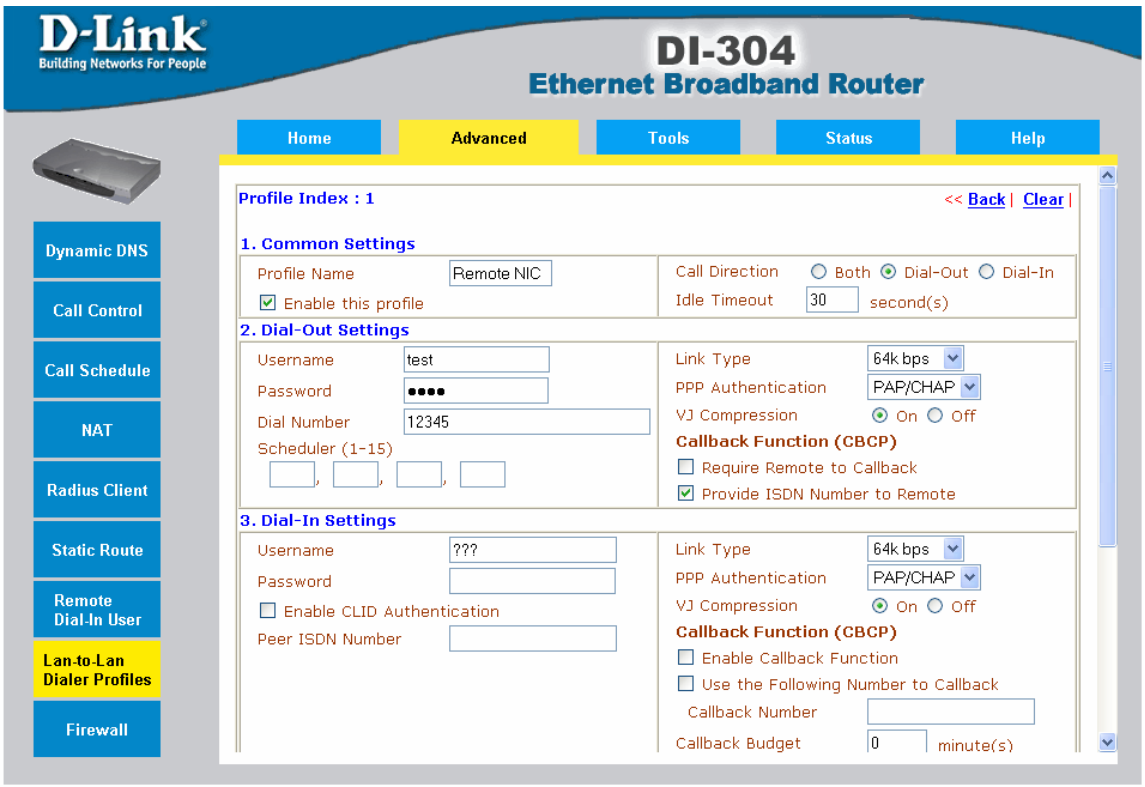

Abbildung 27: Konfigurieren des lokalen LAN-to-LAN Profils (1)

4. Um eine automatische Anwahl zu ermöglichen, muss der IP Adressbereich des entfernten Netzwerks angegeben werden (Abbildung 28). Sollen mehrerer Standorte miteinander vernetzt werden so ist es auch möglich, weitere LAN-to-LAN Profile zu erstellen. Dabei ist es wichtig, dass den verschiedenen Teilnetzen unterschiedliche IP Adressbereiche zugewiesen werden.

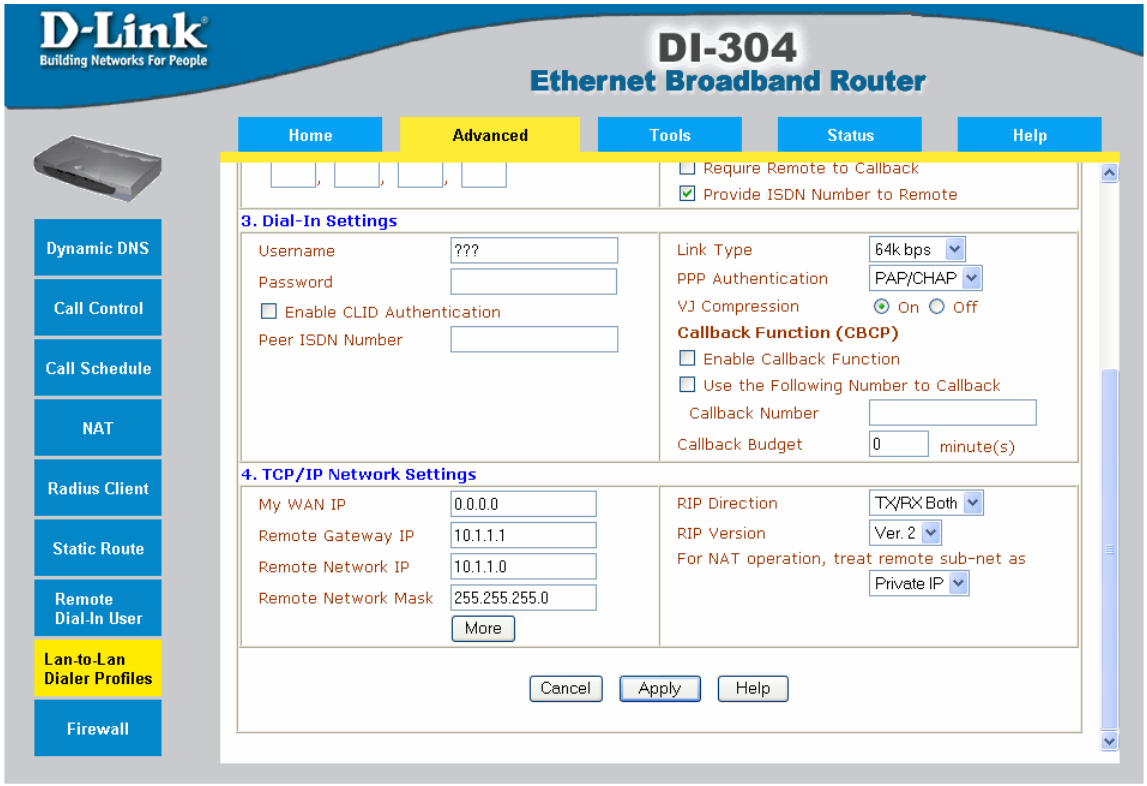

Abbildung 28: Konfigurieren des lokalen LAN-to-LAN Profils (2)

5. Die IP und ISDN Konfiguration des entfernten ISDN Routers ist in Abbildung 29 und Abbildung 30 dargestellt.

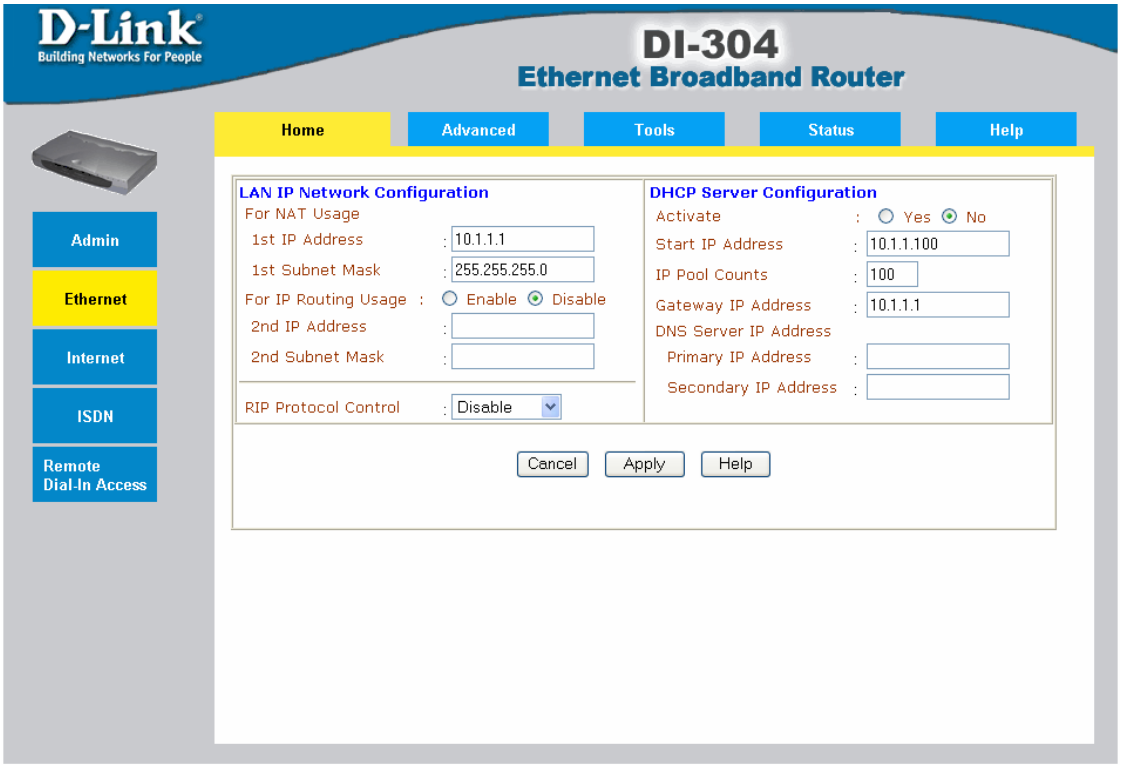

Abbildung 29: IP Konfiguration des entfernten ISDN Routers

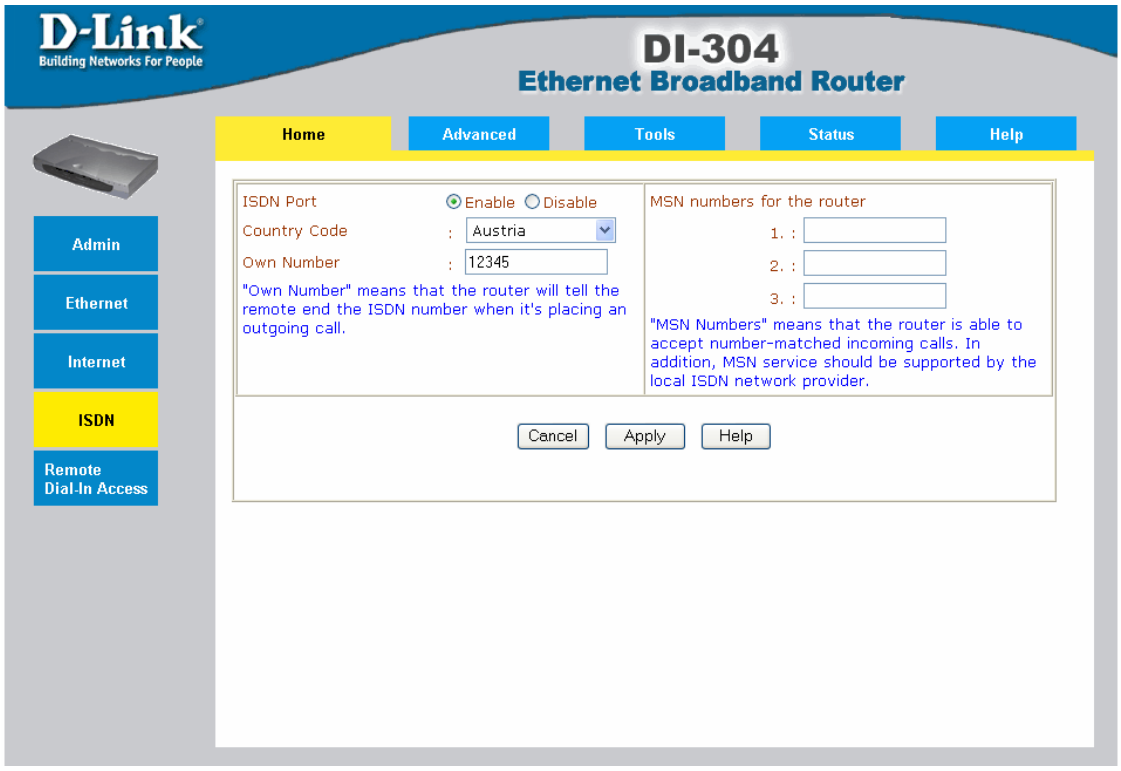

Abbildung 30: ISDN Konfiguration des entfernten Routers

6. Auch in diesem Router muss ein LAN-to-LAN Profil aktiviert werden (Abbildung 31).

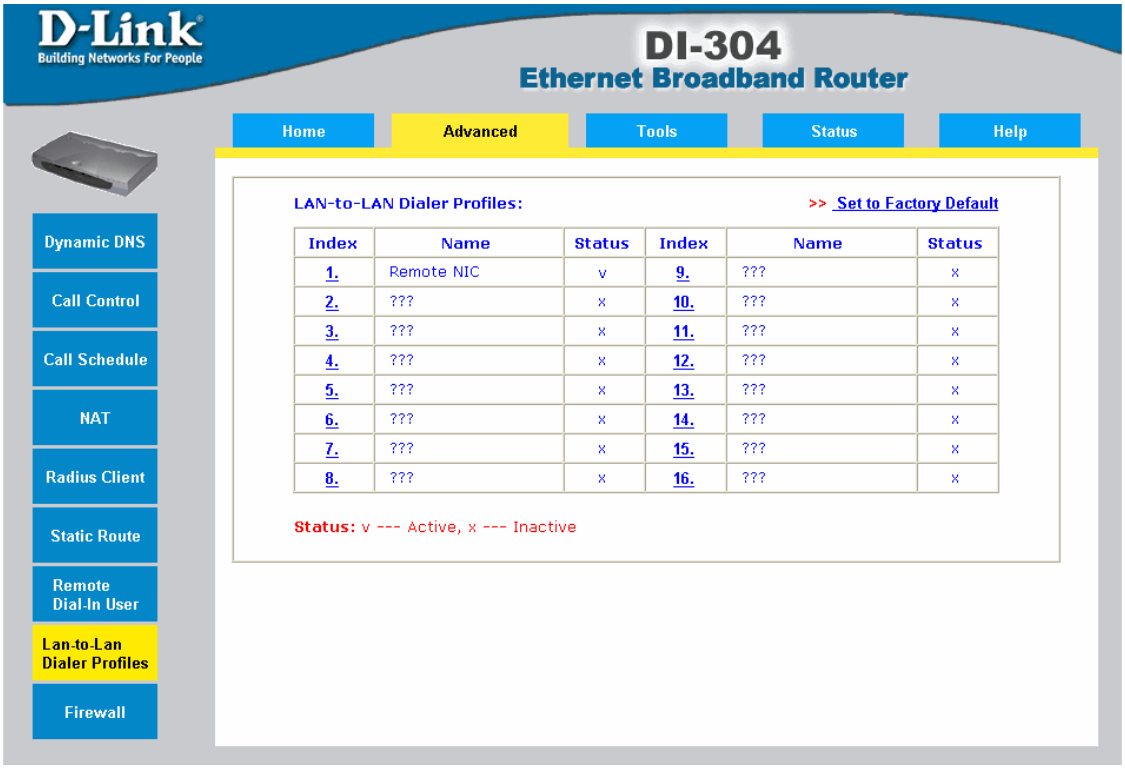

Abbildung 31: LAN-to-LAN Profil des zweiten Routers

7. Benutzernamen und Passwort müssen mit den Einstellungen im lokalen LAN-to-LAN Profile übereinstimmen. (Abbildung 32).

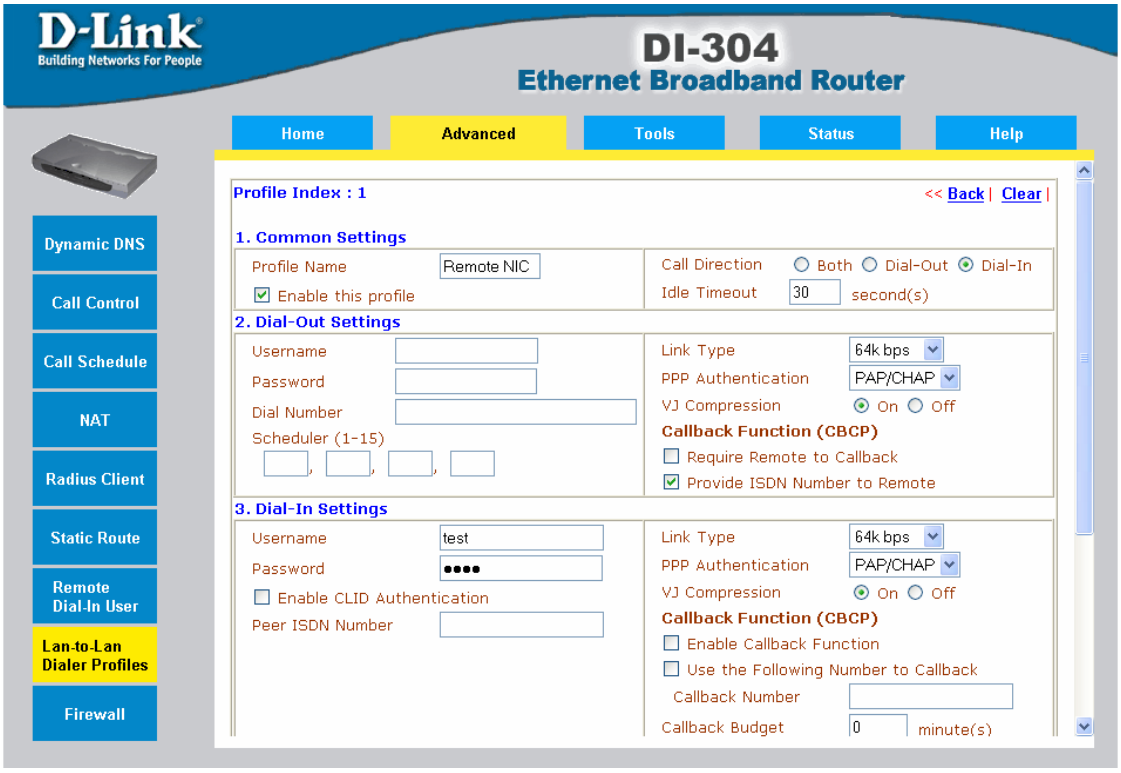

Abbildung 32: LAN-to-LAN Einstellung des zweiten ISDN Routers

8. Abschließend müssen die IP Einstellungen im LAN-to-LAN Profile vorgenommen werden, so dass diese den Bereich des lokalen IP Netzwerks angeben. (Abbildung 33).

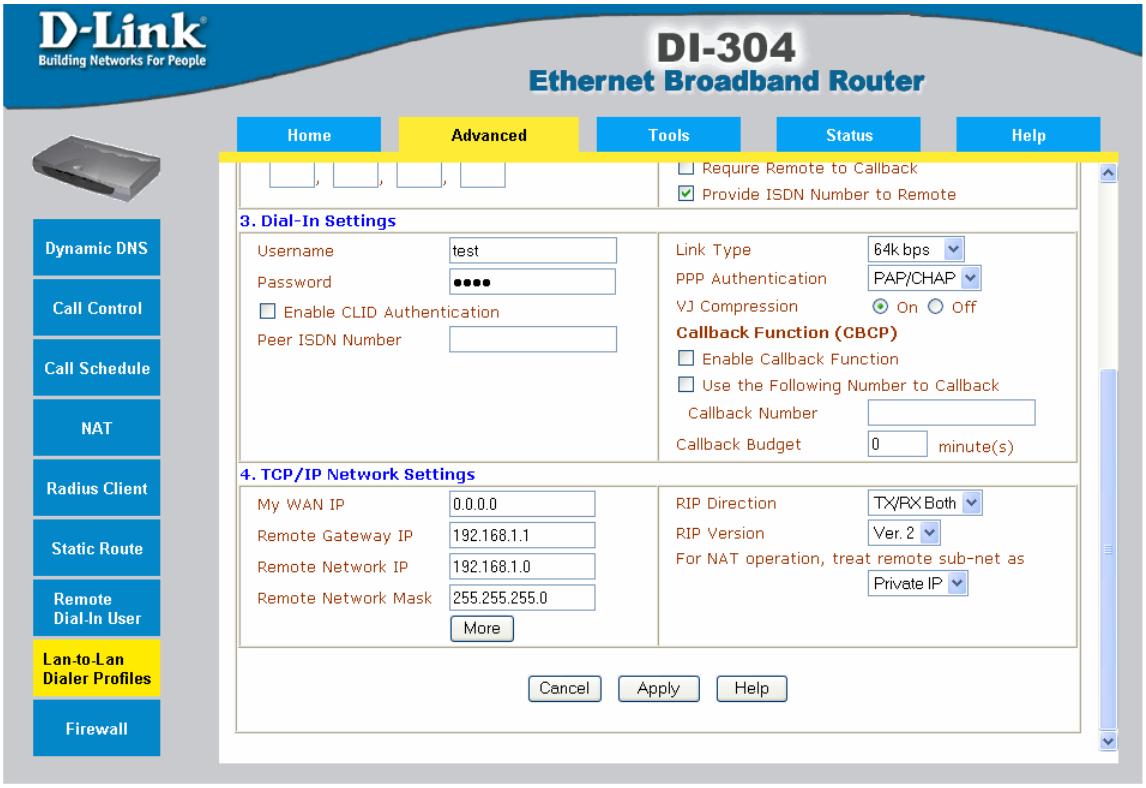

Abbildung 33: LAN-to-LAN Profileinstellungen des zweiten ISDN Routers (2)

In der beschriebenen Konfiguration baut der Router automatisch eine ISDN Verbindung auf, wenn ein Paket an ein Gerät im entfernt liegenden Netz gesendet wird. Dies ist zum Beispiel der Fall, wenn ein entferntes NIC709-IP Interface geöffnet wird. Nach 30 Sekunden Inaktivität auf der ISDN Anbindung wird die Verbindung automatisch abgebaut.

9.2 Einwahlanbindung

Eine ähnliche Konfiguration kann zum Einrichten einer Einwahlverbindung verwendet werden. Anstatt zwei ISDN Router zu verwenden, muss dabei der lokale Router durch eine ISDN Karte im PC ersetzt werden. In Abhängigkeit von der PC Software wird dabei zumeist eine manuelle Aktivierung der Verbindung erforderlich sein.

10 Glossar

Dieser Abschnitt definiert die in diesem Dokument verwendeten Fachbegriffe.

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

- Ein **Gerät** (Device) ist ein einzelner Knoten in einem Netzwerk. Ein Gerät kann Anwendungen (z. B. Lichtsteuerung, Klimasteuerung,…) abarbeiten. Auch

Netzwerkinfrastrukturkomponenten sind Geräte. Ein Gerät kann mehrere Netzwerkanschlüsse (Ports) haben.

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

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

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

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

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

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

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

- **Kanaltypen**:

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

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

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

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

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

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

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

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

- Der **Configuration Server** verwaltet die Information über den Zusammenhang zwischen EIA-709.1 Adressen (Doman, Subnet, Node, Router Type,…) und IP

Adressen auf einem IP-852 Kanal. Pro IP-852 Kanal darf nur ein Configuration Server aktiv sein. Ein Server kann auch mehrere Domains verwalten.

11 Referenzen

[1] LonMark Interoperability Association: LonMark Layer 1-6 Interoperability Guidelines, Version 3.4, September 2005

[2] Echelon Corporation: LonWorks FTT-10A Free Topology Transceiver Users's Guide, Version 6, 2001

[3] LOYTEC electronics GmbH: Anwendungshinweis AN006G L-Switch und LNS, Document Number 86001104

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

[5] LonMark Deutschland e.V..: LonWorks Installationshandbuch, VDE Verlag GmbH, 2. Auflage, 2004

[6] L-IP Benutzerhandbuch, LOYTEC electronics GmbH, Version 4.5, Document Number 88066009.

[7] LOYTEC electronics GmbH: Anwendungshinweis AN008G, Netzwerk Fehleranalyse White Paper, Document Number 86001501

12 Warenzeichen

13 Versionsübersicht

Datum	Version	Autor	Beschreibung
2004-04-30	1	NR	Erste Version
2005-06-17	2	NR	Kapitel über ISDN Anbindung hinzugefügt Ergänzungen für L-IP33ECTB
		NR	Limit von 6 Domains pro CS entfernt (nicht mehr gültig!)

2006-12-04	3	NR	Entfernen des Colissionless Backbone Modus L-IP 3333ECTB ergänzt Erklärungen zu L-IP und NAT Router hinzugefügt Erklärungen zu NIC-852 hinzugefügt Beschreibung von L-Proxy an LP-33E100 angepasst.
2006-12-05		DAD	Grafiken an die neue Hardware angepasst. Bei Grafiken mit L-Switch das "B" hinzugefügt. Tabelle 2: kollisionsfreier TP/XF-1250 entfernt. Kapitel 8: "Bedeutung" einer roten LED eingefügt. Kapitel 8: LSD-Tool vor LPA-Tool geschoben - Referenz: [1] LonMark Interoperability Association: LonMark Layer 1-6 Interoperability Guidelines, Version 3.4, September 2005 (Aktuelle Version) - Referenz: [3] LOYTEC electronics GmbH: Anwendungshinweis AN006G L-Switch und LNS, Document Number 86001104 (Aktuelle Version)