1 Introduction

This application note provides information on how to use LOYTEC network infrastructure products (L-Switch, L-Switch XP, L-IP and L-Proxy) together with LOYTEC network interfaces in different example uses cases. It also explains how the different operating modes of the devices work and which operating mode should be chosen for specific applications. It addresses as well the issue of protocol analyzing and system diagnostics in the network"

2 Why should I structure my Network?

With the increasing size of EIA-709 installations, also the complexity of these installations increases. There are several technical, but also practical reasons why such networks need a structured network layout:

- Maximum number of nodes on a channel: The specifications of transceiver types [2] as well as the LonMark Interoperability guidelines [1] specify the maximum number of nodes, which may be physically connected to a single network channel. The number of nodes depends on the transceiver type. As an example, the maximum number of TP/FT-10 based nodes on a single network segment is 64 nodes. If the number of nodes in the network exceeds this limit, the network has to be divided up into several network segments, connected by network infrastructure products (see Table 1).

- Maximum cable length: The transceiver and LonMark specifications limit the maximum cable length per network segment. The maximum length depends on the transceiver type as well as the network topology (bus, free topology, see Table 1).

- Reduce Network Traffic: With increasing number of nodes in a network, also the amount of data, which is exchanged between the nodes, increases. To avoid overload situations on the network, network infrastructure components like routers and switches can be used. These components filter the packets on the network, depending on the destination address.

- Increase Reliability: Switches and routers are filtering noise and bad packets (this is, packets with invalid content or CRC errors) on the network. If a packet is corrupted, e.g. due to noise on the network, it is discarded rather than forwarded by the router or switch. This allows keeping the overall performance of the network in a good condition even if there are problems in some network segments.

- Increased Maintainability: Structured networks allow isolating single channels for maintenance purposes without influencing the rest of the network. LOYTECs L-IP devices even allow to connect the LOYTEC Protocol Analyzer remotely via an IP-852 (Ethernet/IP) channel to channels (TP/FT-10, TP/XF-1250, RS-485) behind the L-IP router to perform protocol analysis on those channels. Even an Intranet or the Internet can be used since the communication on an IP-852 channel is based on the IP protocol.

3 Electrical Characteristics

3.1 Channel Type

Channel Type	Cable Length and Cable Type	Nodes per Segment
TP/FT-10 (Bus)	CAT5 Cable: 900m (max. Stub = 3m)	64 (128 for Link Power Transceiver)
TP/FT-10 (Free Topology)	CAT 5 Cable: 450m Max. Device-Device distance: 250m	64 (128 for Link Power Transceiver)
TP/XF-1250	Cat 5 Cable: Typ. 500m Worst Case 130m Max. stub length 0,3m	64 (0 to +70°C) 32 (-20 to +85°C) 20 (-40 to +85°C) <=8 devices per 16m section
IP-852	Ethernet 10BaseT	256

Table 1: Standard channel specification [1]

3.2 Termination

For the correct operation of the network, each network segment has to be terminated properly according to the channel specification.

Note: On multi-port devices, also unused ports have to be terminated properly!

3.2.1 TP/XF-1250

The TP/XF-1250 uses transformers for galvanic isolation. The topology of a TP/XF-1250 channels is a bus. Thus, both ends of the bus cable need to be terminated with a termination network as shown in Figure 1.

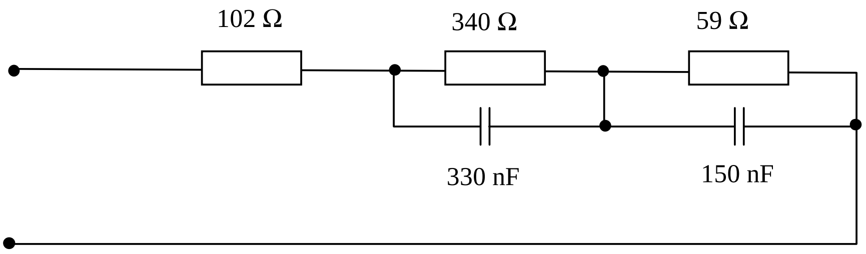


Figure 1: TP/XF-1250 Termination Network

3.2.2 TP/FT-10

TP/FT-10 ports can also be used on Link Power (LP-10) channels. When using the Free Topology Segment feature of the TP/FT-10, only one termination (Figure 2) is required and can be placed anywhere on the free topology segment.

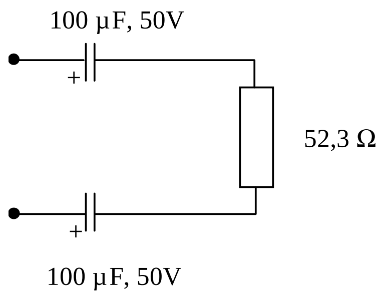


Figure 2: TP/FT-10 Free Topology Termination

In a double terminated bus topology, two terminations are required (Figure 3). These terminations need to be placed at each end of the bus.

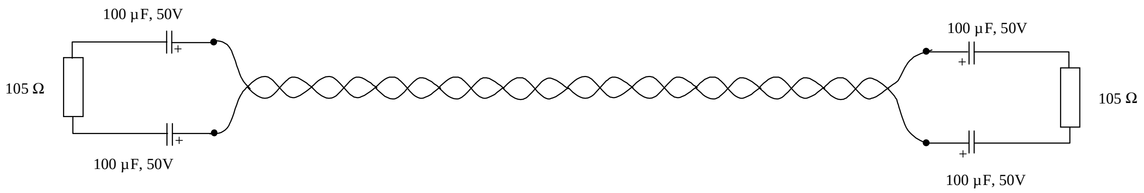


Figure 3: Termination in a TP/FT-10 Bus Topology

3.3 Bandwidth Utilization

Table 2 shows the maximum packet throughput on selected channel. To avoid collisions on the channel, the maximum channel bandwidth utilization must not be higher than approx. 70%.

Channel Type	Maximum Packets/s (approx.)
TP/FT-10	200-250
TP/XF-1250	600-800
IP-852	600

Table 2: Maximum packet throughput on selected channels

4 Typical Network Structures

4.1 Backbone Channels and Local Channels

In most networks the network traffic can be divided into two parts:

1. Local network traffic. This traffic includes all messages, which are exchanged between nodes, which are located in a rather small area like an office room or a single floor within an office building. Local data include control commands to switch on and off lights, sensor and control data for HVAC applications (e.g. temperature) or the manual control of sun blinds.

2. Global network traffic. This traffic describes all messages which are exchanged between local nodes and more centralized nodes, like a SCADA System, LNS Server, OPC Server or a weather station node. Global network traffic includes network management and diagnostics as well as the data exchange between the nodes and the SCADA system.

The two network traffic types build the basis for the network infrastructure design. Rather small network segments, which process the local network traffic, are connected by network infrastructure components to a high speed backbone channel, today normally an IP-852 (Ethernet/IP) channel. The network infrastructure components keep the local network traffic in the small segments and do not forward the traffic to the backbone. On the other hand, the global network messages are forwarded from the nodes on the backbone only to those local segments, which host the destination nodes for the messages. Figure 4 shows such a network structure.

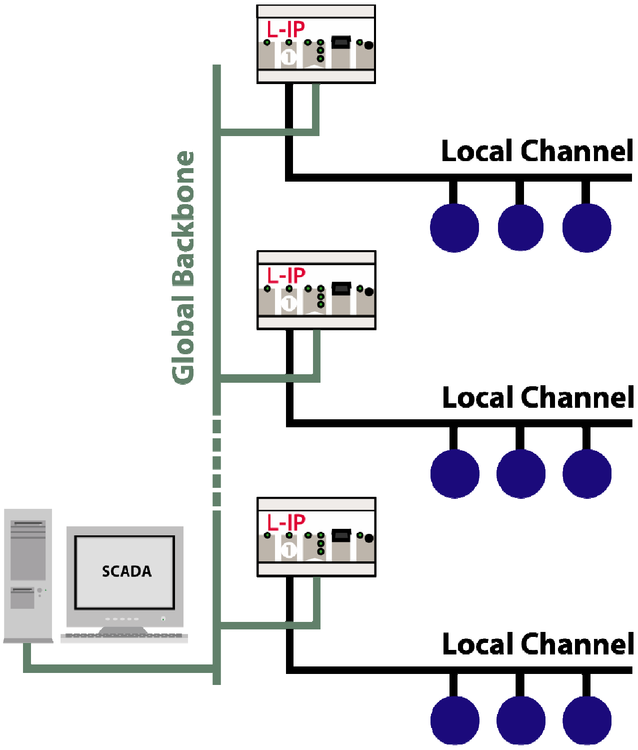


Figure 4: Local Channels, connected via a global Backbone

The transceiver type for the local channels has to be selected to match the transceiver type of the field devices – in many cases this will be TP/FT-10 – whereas the channel type of the backbone can be a TP/XF-1250 or TP/FT-10 channel beside an IP-852 (Ethernet/IP) Channel depending on the required channel bandwidth and cabling requirements of the specific application.

4.2 Low Speed Backbone Channel (TP/FT-10)

In small networks the available bandwidth of a TP/FT-10 channel (78 kbit/s) might be enough to meet the requirements for the backbone channel. The example in Figure 5 shows a network using a TP/FT-10 backbone channel. Different types of L-Switch devices connect the local channels to the backbone. The L-Switch device can be chosen depending on the number of local channels, which are needed in a design unit (e.g. a single floor in an office tower) for the local channels.

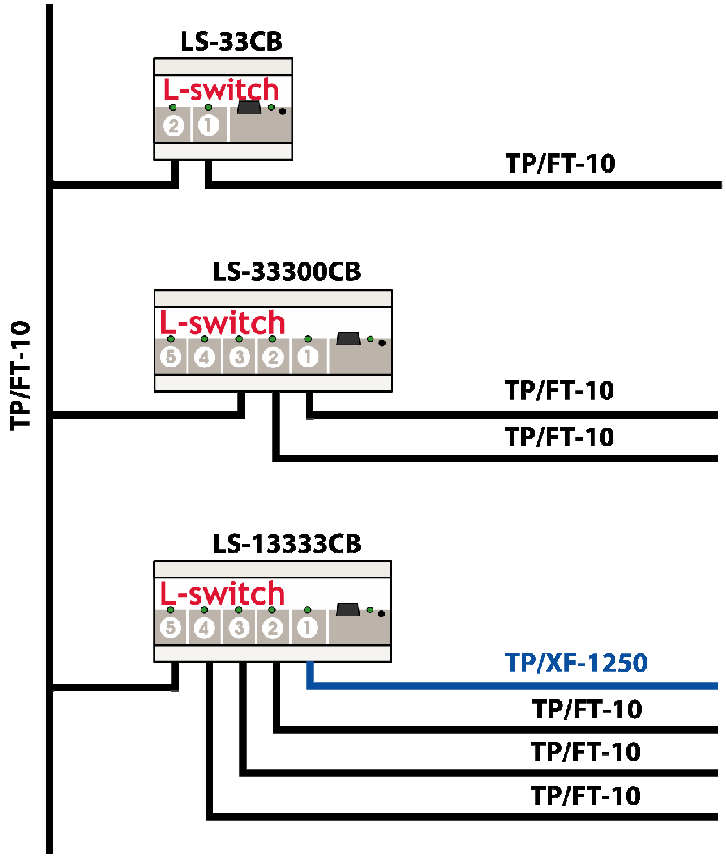


Figure 5: Network with TP/FT-10 backbone channel

4.3 Backbone with TP/XF-1250 in normal mode

For most applications the backbone is required to allow a higher network throughput than it is required for the local channels. In many cases the TP/XF-1250 channel (1,25 Mbit/s) provides enough bandwidth to meet these requirements. Figure 6 shows a network with a TP/XF-1250 backbone. The L-Switch router of type LS-1xxxxC connects one port to the TP/XF-1250 backbone and one or multiple TP/FT-10 channels for the local network segments.

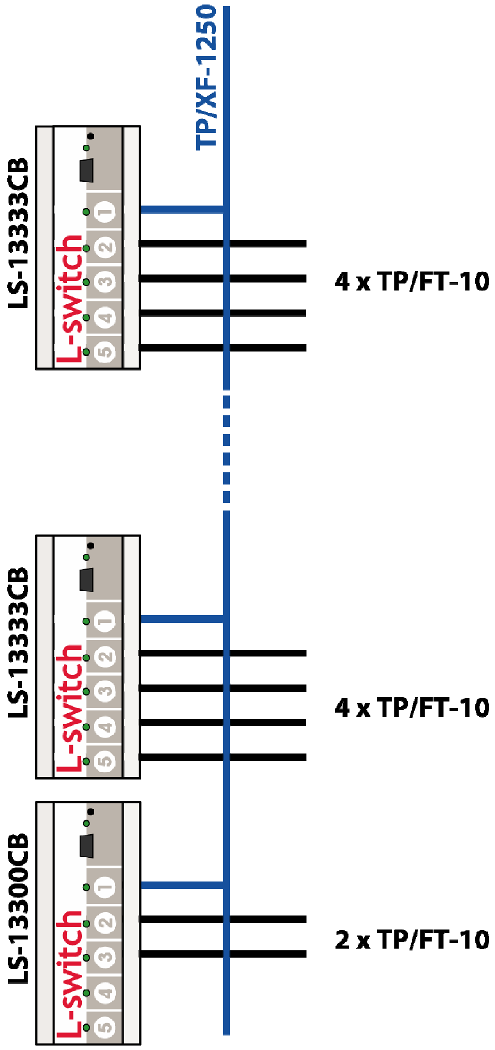


Figure 6: Network with TP/XF-1250 backbone channel

If the backbone has to be extended because the cable length exceeds the specification limits for TP/XF-1250 channels, the network structure in Figure 7 can be used.

Note: It is recommended to extend the backbone not more than 5 times.

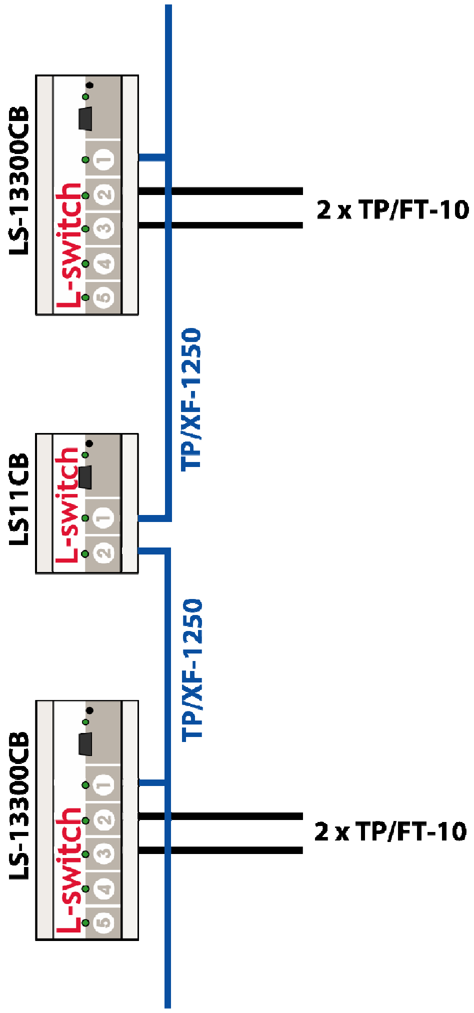


Figure 7: Network with TP/XF-1250 backbone channel. The backbone channel is extended with an LS-11C.

4.4 IP-852 Backbone Channel

More and more Ethernet/IP becomes accepted as a transmitting medium for a IP-852 Backbone channel. As a future-proofed communication technology Ethernet/IP offers an extremely high data transmission rate and also flexible access on the entire network from a central point. With the use of the appropriate IP network infrastructure communication is possible both over an Intranet and over the Internet.

IP-852 channels require a configuration server to build the channel. L-IP devices have a built-in configuration server. The server must be activated on exactly one L-IP per IP-852 channel. The IP addresses of all channel members have to be added to the channel member list in the configuration server. The configuration server (CS) manages the mapping between the domain/subnet/node and group addresses and the IP addresses of the channel member devices. Whenever the network configuration is changed, the channel member device sends a configuration update message to the configuration server (see blue arrow in Figure 8). The configuration server forwards the update packet to all channel members (see red arrow in Figure 8). A single L-IP configuration server can handle up to 256 channel member devices whereas the channel members can be configured in different domains.

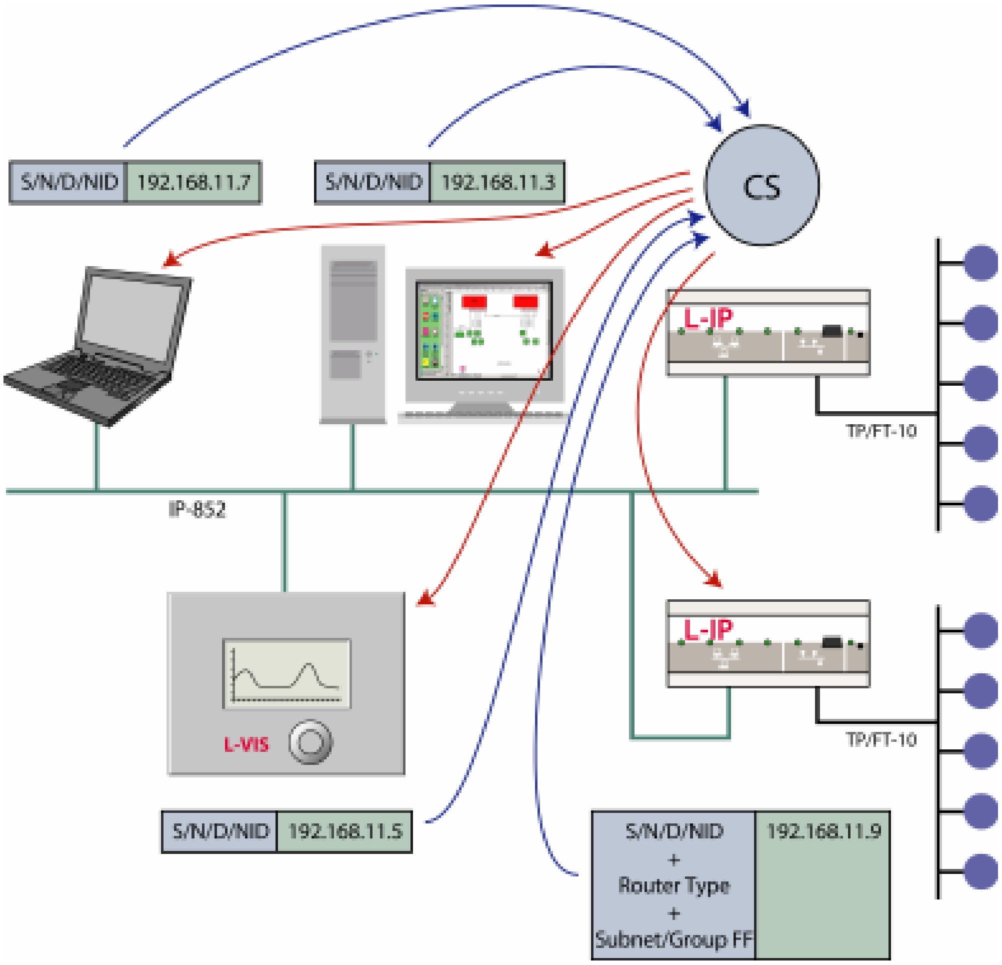


Figure 8: Configuration server for IP-852 channels

For networks, which need high performance, highly flexible network structures, remote maintenance, and analysis capabilities, the backbone channel built by an IP-852 channel is the best solution (Figure 9). The L-IP router connects to the IP-852 Ethernet channel on one side and to the local TP/FT-10 channel on the other side.

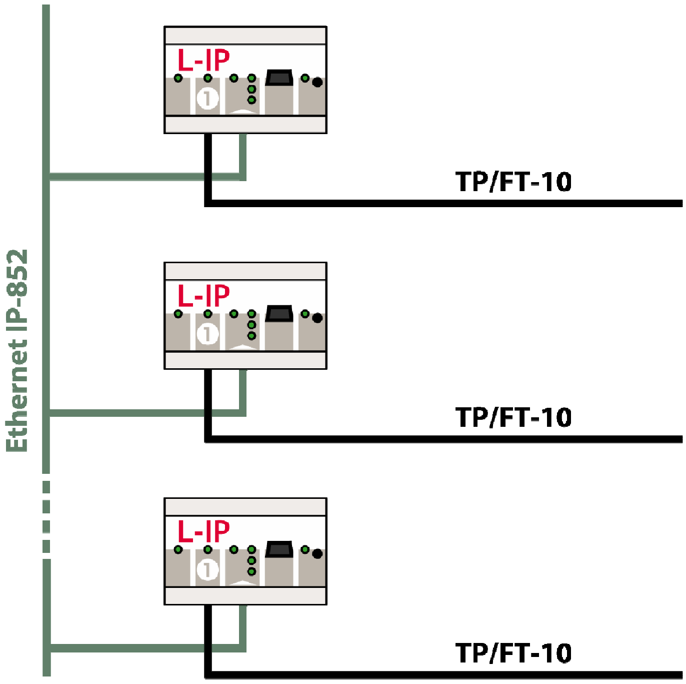


Figure 9: IP-852 backbone with local TP/FT-10 channels

If more than one TP/FT-10 channel is required in a local network segment but the advantages of IP-852 backbones are needed, multiport L-IPs (Figure 10) can be used. The big advantage of IP-852 backbones is, that the existing Ethernet network infrastructure can be reused, which may save cost when extending an existing network. An IP-852 backbone channel can also spread across multiple buildings. If a SCADA system is connected to the IP-852 backbone, the network in all buildings can seamlessly be monitored by one SCADA system (see Figure 11).

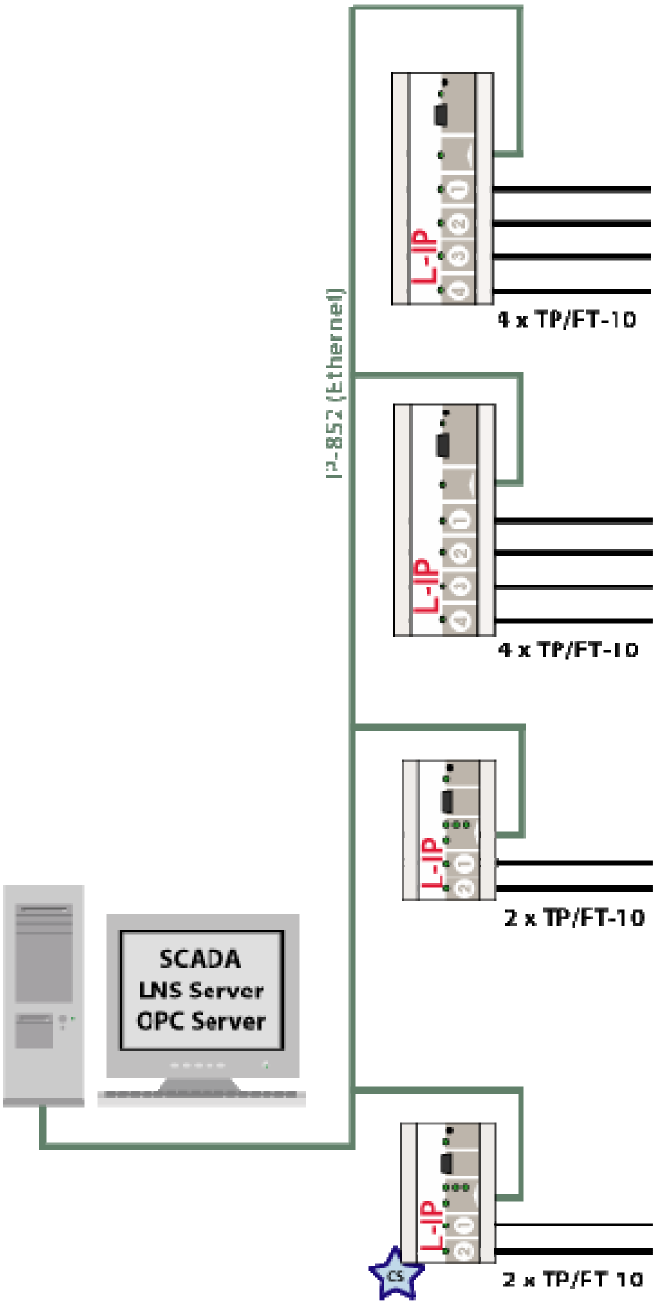


Figure 10: Connect multiple FT-10 channels with multiport L-IP

The advantage of the IP-852 backbone shown in Figure 9, Figure 10 and Figure 11 over the TP/XF-1250 backbone is that the L-IPs can also be used as a network interface for remote network analysis. Read the section Remote Network Analysis and Maintenance to learn more about this topic.

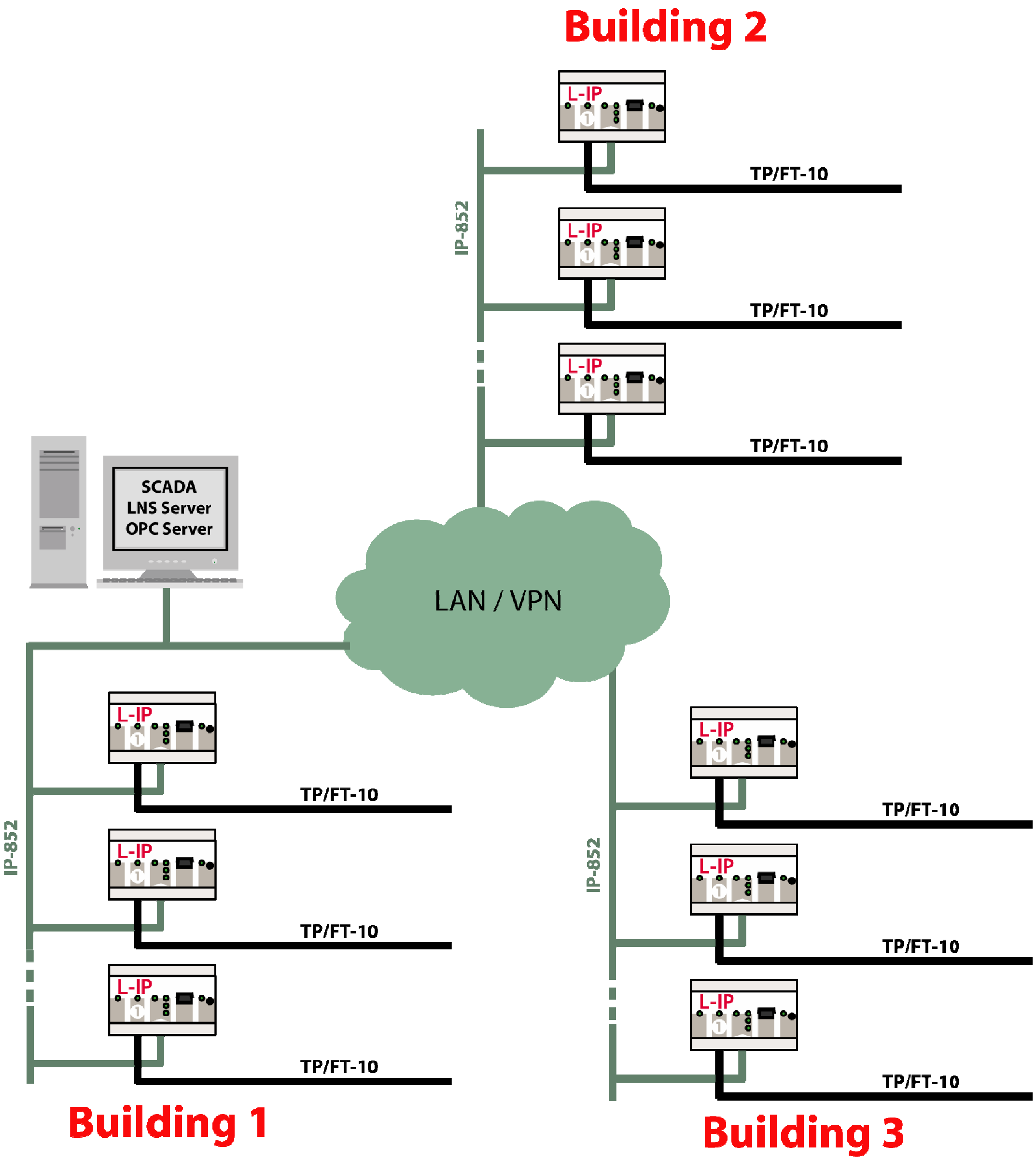


Figure 11: Using an IP-852 backbone across multiple buildings in order to monitor all 3 buildings from one SCADA system.

Concerning the transmission rate, flexibility and reliability, an IP-852 backbone channel as shown in Figure 10 and Figure 11 is the optimal solution and preferable compared to all other variants to build a flat network hierarchy.

Another possibility is the combinations of IP-852 backbones and TP/XF-1250 backbones to connect e.g. multiple buildings to a single system. In that case an existing Ethernet connection between the buildings could form the link via an IP-852 channel between TP/XF-1250 backbone channels in the buildings (see Figure 12). In the example, a SCADA system for all buildings is connected to the TP/XF-1250 backbone in Building 3.

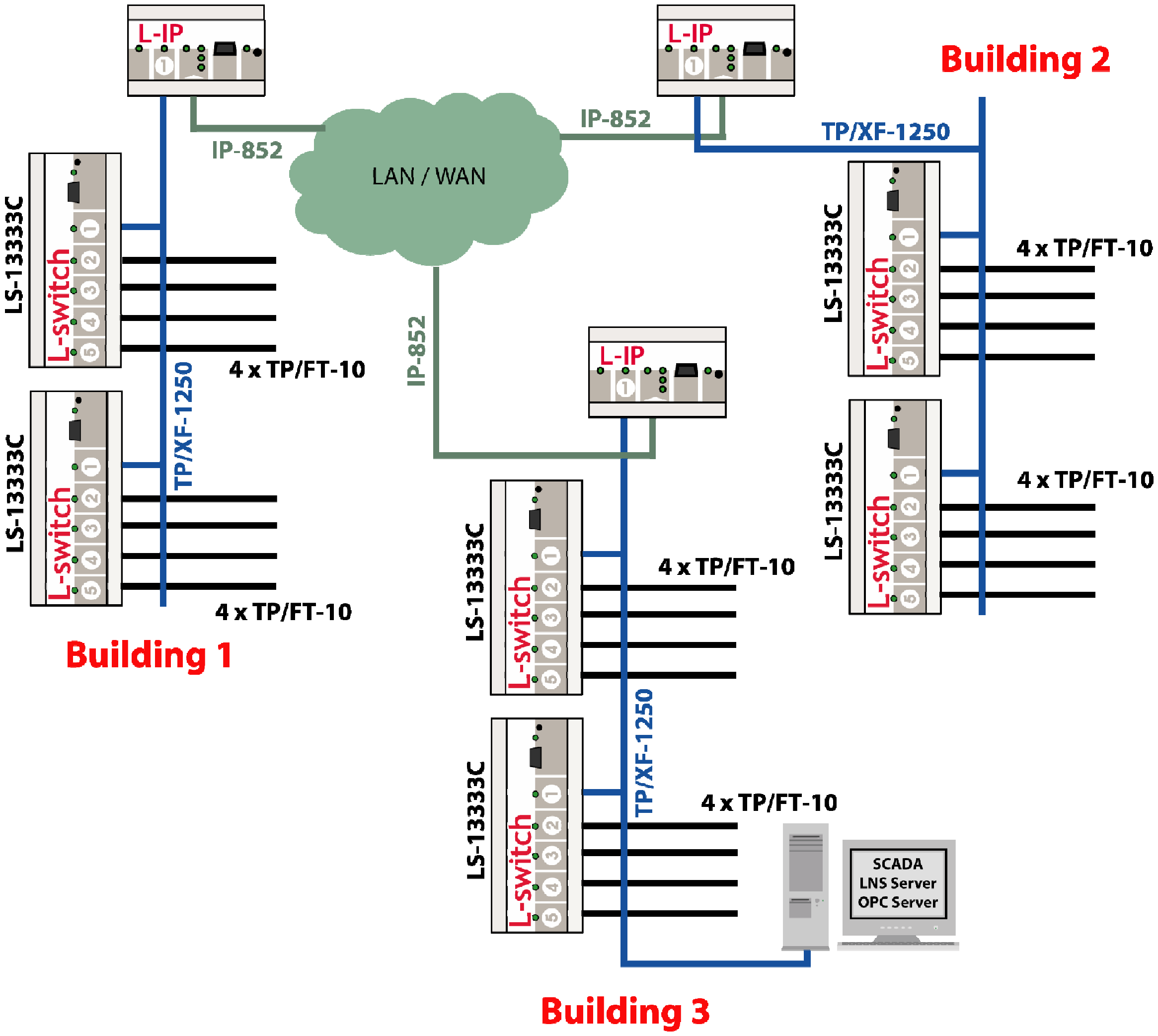


Figure 12: Connecting multiple buildings over IP-852 channel, using TP/XF-1250 backbones inside the buildings.

5 Distributed networks with (NAT) firewalls and dynamic IP addresses

In networks which span several locations via an IP-852 channel, the different locations often are protected by a firewall. Mostly the firewall includes a NAT (Network Address Translation) router which represents the network behind the router by a single public IP address. The use of IP-852 devices behind a NAT router has an essential impact related to the usability and configuration. These relations are described in this section in detail. In the following chapter the terms „NAT Firewall "and „NAT router" are used synonymously.

5.1 Operation of a L-IP behind a NAT firewall

As described in the preceding chapters the data exchange on the IP-852 channels takes place by sending packages from an IP-852 node to the IP address provided by the configuration server. Unlike to a local network the IP address of a target node behind a NAT firewall is not directly reachable. As shown in Figure 13 the L-IPs are 'hidden' behind the firewalls.

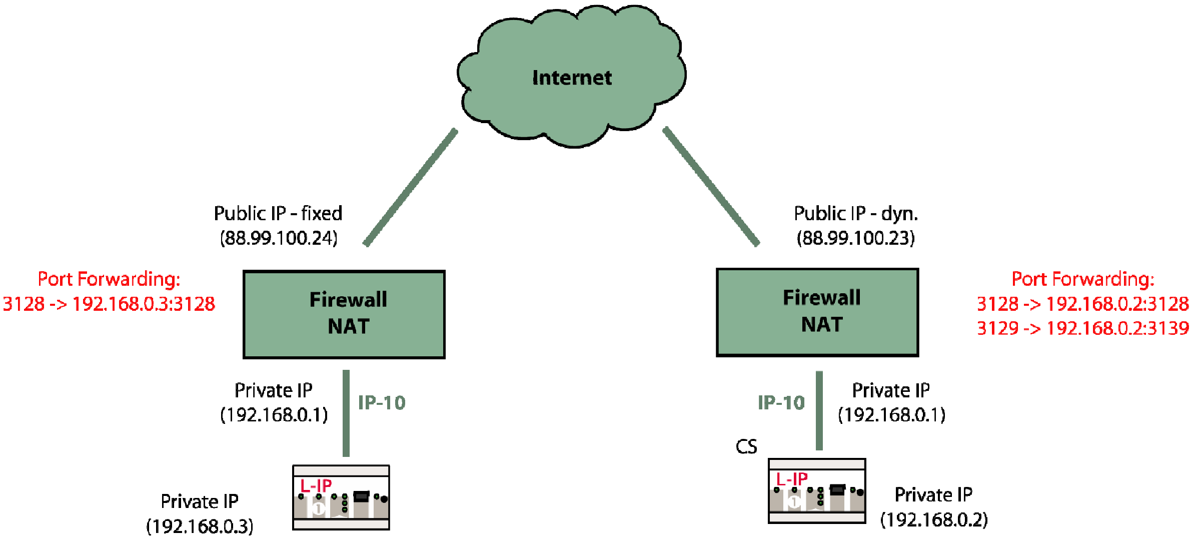


Figure 13: Single L-IPs behind NAT firewalls

The NAT firewall has two addresses: A public address about which it is reachable from the public network as well as a private IP address where the NAT router is reachable from the local network. Normally this local address is entered as the standard gateway in the local network. To reach an LIP behind the firewall a node on the IP-852 channel first must send a package to the public address of the firewall visible from the outside. Within the firewall a port forwarding rule is defined defining to what internal, local address an external package received on a specific port has to be forwarded.

If e.g. the left L-IP in Figure 13 wants to send a package to the right L-IP, the package has to be sent to the public IP address of the right firewall (88.99.100.23) on Port 3128.

The right firewall decides based on the port forwarding rule that this package has to be forwards to the L-IP (192.168.0.2, Port 3128). For the server port of the configuration server the port forwarding rule is defined in the same way. The configuration server then must be configured in the way that the IP address and the client port number of the L-IP as well as the public address of the NAT firewall (NAT address) where the L-IP is connected to, is registered. Details about how to configure the configuration server can be found in [6].

5.2 Operation of several L-IP behind a NAT firewall

If several L-IPs are connected to one NAT firewall, the L-IPs must be adjusted to different client ports, following the port forwarding rules defined within the NAT firewall (see Figure14). In the described example all packages received by the right firewall on port 3120 of its public address are forwarded to the private IP address 192.168.0.2, port 3128. Packages on port 3130 are forwarded to the private IP address 192.168.0.3, port 3130.

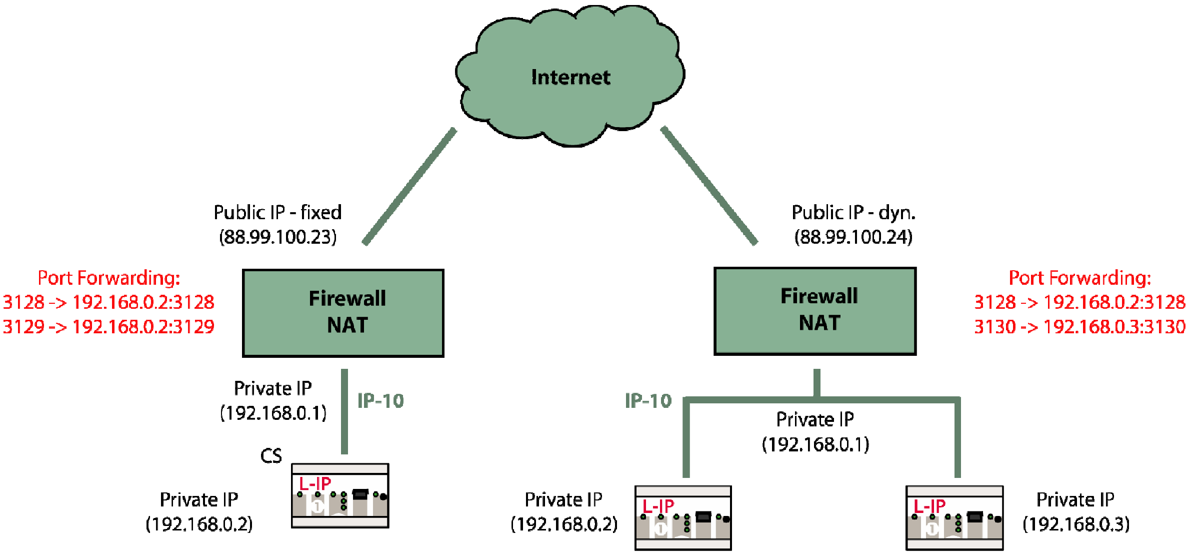


Figure14: Operating several L-IPs behind a NAT firewall

The configuration server is switching to the ‘Extended NAT’ mode if there are at least 2 L-IPs on an IP-852 channel behind a NAT firewall. In this mode packages with other L-IPs and LOYTEC products can be exchanged, but not with IP-852 router from other manufacturers.

5.3 Operating a PC behind a NAT firewall

It is also possible to operate a PC on an IP-852 channel behind a NAT firewall. For that purpose a NIC-852 network interface is needed for the PC (Figure15). Beside the IP address of the configuration server the public IP address of the NAT router (88.99.100.22), where the PC is connected to, must be entered in the configuration software of the NIC-852. The port forwarding rule must be defined within the NAT router like described for the operation of a L-IP behind a NAT firewall.

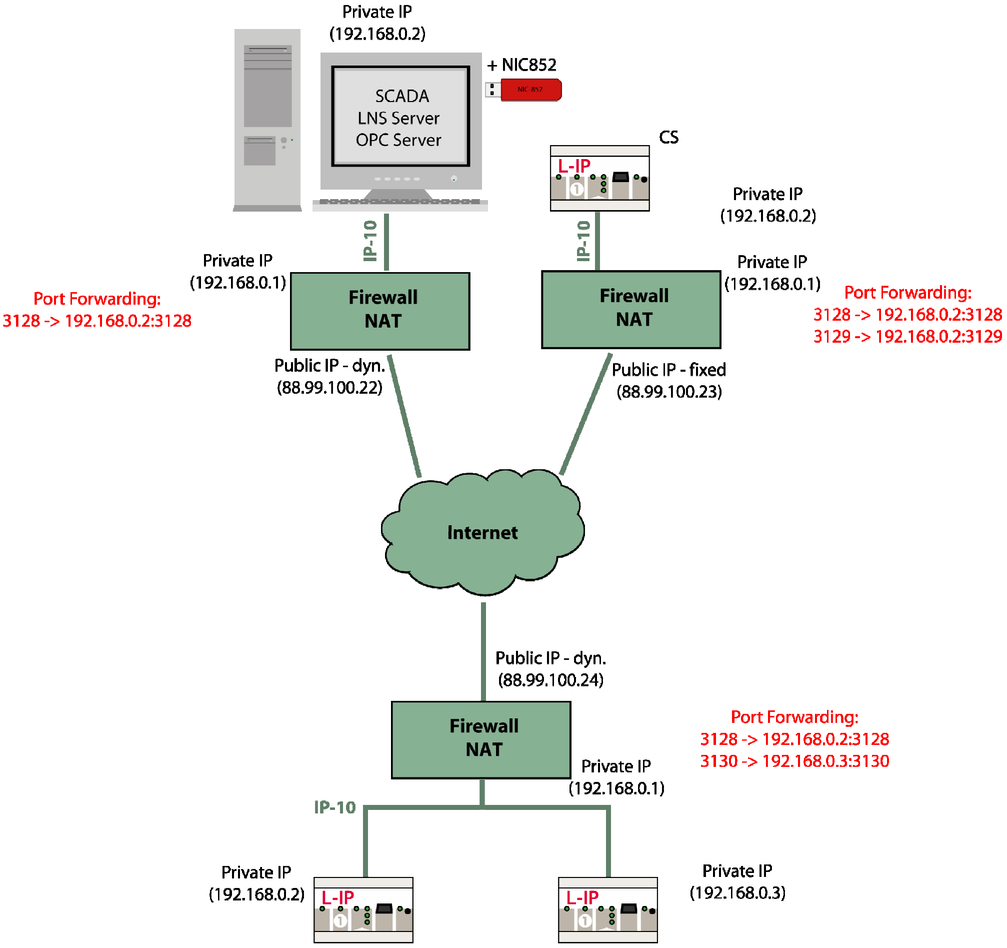


Figure15: PC with NIC-852 behind a firewall

5.4 Operating with dynamic IP addresses

Within a building network the devices on an IP-852 channel (L-IP, PC, L-VIS, …) mostly get static IP addresses, because these devices are attached to the building with a permanent location.

For NAT firewalls it often happens that the public address of a NAT router is dynamically assigned. Thus it can happen that the IP address is changing during the operation. This change of the IP address needs to update the channel member list in the configuration server. The configuration server then distributes the new IP address to the other channel members on the IP-852 channel. Doing this manually is practically not possible. Therefore the L-IP configuration server option ‚Roaming Member’ allows the configuration server to detect changed IP addresses, update the channel member list and distribute the new IP addresses to all other channel members. One or several devices can be operated on a channel behind a NAT router with a dynamic IP address. The only limitation is referring to the IP address of the NAT router where the L-IP with an enabled configuration server is connected to. This IP address must be a static IP address since the configuration server must be always reachable by the channel members.

6 Smart Switch Mode vs. Configured Router Mode

The L-Switch XP devices and the L-IP allow choosing between two operating modes. In the smart switch mode, the device learns the network topology from the traffic on the network automatically. In the configured router mode, the network management tool writes the routing tables during the configuration of the network. Changes on the network always require the network management tool to alter the routing tables in the router devices. Table 3 shows the available modes for the different devices together with the factory default configuration.

Device	Smart Switch Mode	Router Mode
L-Switch	Yes (default)	No
L-Switch XP	Yes (default)	Yes
L-IP	Yes	Yes (default)

Table 3: Device types and default configuration

6.1 Smart Switch Mode

In the smart switch mode, the device learns the network structure from the packets, which are received on the network and forwards the packets according to the already learned configuration. For the learning and forwarding mechanism, it applies that the

- address is **learned** from the **source** address of the packet and the packet is
- **forwarded** according to the information in the **destination** address of the packet.

Packets, which are addressed to destination addresses, which have not been learned yet, are always forwarded to all ports except the port on which the original packet was received. The learning algorithm is able to learn subnet/node addresses as well as group addresses. Because the network configuration is always learned from the source address of a packet, subnet/node addresses can only be learned for nodes, which actively send out packets. If a node never sends a packet but always received messages, the address of this node can not be learned and therefore packets which are sent to this node will always be flooded to all ports of the device. Please note that for the learning algorithm it is sufficient to receive acknowledgement packets. This means that having acknowledged communication between two nodes already assures that the subnet/node addresses of both nodes are learned. Since several messages are exchanged between the nodes on the network and the network interface of the network management tool during the commissioning phase, the network structure in most cases is already learned after the installation process.

To learn group addresses, it is required that at least one message in the group is sent out using acknowledged service. Using only group communication in unacknowledged or unacknowledged repeated service results in that the group messages are flooded to all ports of the learning device.

To use the device in smart switch mode, the device **must not be commissioned** in the network management tool. However, for documentation purpose or to connect nodes across different channel types, router devices can be used in the network management projects. Please refer to [3] for more information on that topic.

The network topology ‘Loop’ is not possible in the smart switch mode. This means that that a connection between two nodes in a network is only possible on exactly one path.

6.2 Router Mode

In router mode, the device works like a configured router. The network configuration is configured by the network management tool. To accomplish this, the device **has to be commissioned** in the network management project. Only the router mode “Configured router” is valid for the LOYTEC L-Switch XP and L-IP. The devices will report an error if they are configured as a repeater or leaning router device.

6.3 When to use Smart Switch mode? When to use Router mode?

Using LNS® based network management tools the use of the router mode “Configured router” is always recommended. That helps the management tool to identify problems while installing a network, e.g. connecting a node to a wrong channel. For the L-IP devices, the recommended operation mode is the configured router mode because in this mode the resources of the IP network can be used more efficiently.

The Smart Switch mode is recommended when routers are added to an already installed system and if the network structure should not be changed in the network management tool. This mode is also convenient if the management tool can not set the routing table of the router automatically in the right way.

In general, the router mode should be used if there are lots of groups in the network, which use unacknowledged or unacknowledged repeated service. Also in networks, which use subnet wide broadcast messages the configured router mode is the operating mode of choice.

7 Multi-Domain Installations

In ANSI/EIA-709 systems, a single node can communicate with nodes within one single Domain. In network management tools, a domain equals a project in the LNS database. Although in most installations the maximum number of nodes in a domain (32385) is never reached, the limited number of available group addresses (256) can be a serious problem.

A solution for this problem is to divide up the network into multiple domains and use the L-Proxy device to exchange data between the different domains. To accomplish this, the L-Proxy provides 5 ports (2x TP/FT-10, 3x on IP-852 (Ethernet/IP) where each port can act as an independent node. Each port can be commissioned in its own domain. Static, dynamic and external (polled) network variables, which can be created on the L-Proxy ports with a configuration software supplied with the L-Proxy, can be connected internally. That way it is possible to exchange data across domain boundaries.

7.1 Connecting two domains by TP/FT-10 channels

In the simplest case two networks in different domains are to be connected by TP/FT-10 channels like shown in Figure 16.

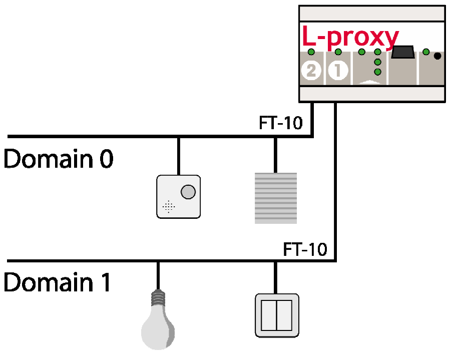


Figure 16: L-Proxy Gateway in a network with two domains.

In this configuration the nodes on the IP-852 (Ethernet/IP) port are not used.

7.2 Connecting 2 to 5 Domains

Up to 5 domains can be connected using one L-Proxy LP-33E100. For the 5 domains three nodes on the IP-852 (Ethernet/IP) channel are available beside the 2 nodes on the FT ports. Like the nodes on the FT ports up to three nodes are installed on the IP-852 channel. It concerns three ‘virtual’ nodes on the same IP-852 (Ethernet/IP) channel but logically separated in three nodes with an independent configuration. To run the IP-852 nodes of the L-Proxy on the IP-852 channel the L-Proxy must be added in the channel list of the configuration server. Only one entry is necessary for one L-Proxy. This entry represents die 3 L-Proxy IP-852 nodes.

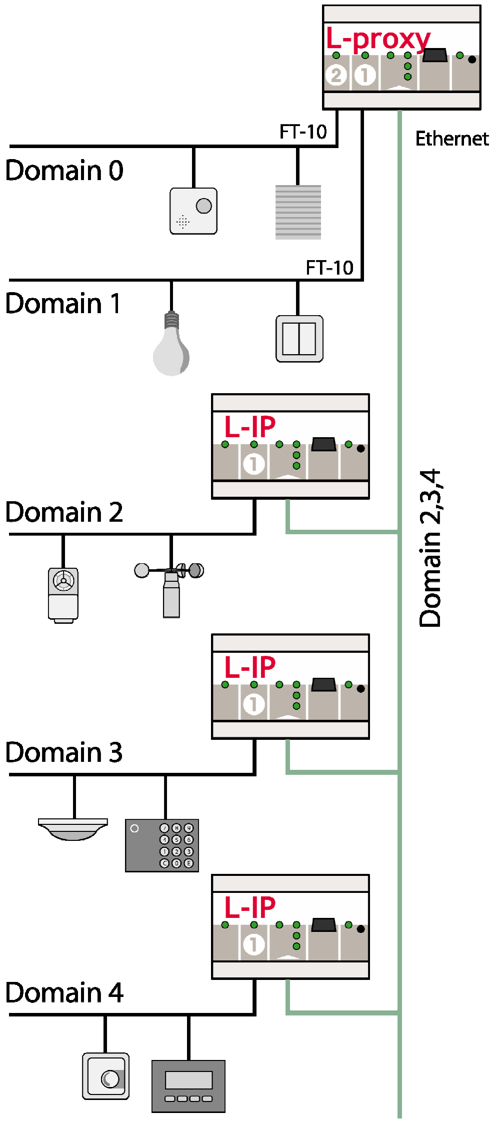


Figure 17: Connection of up to 5 domains with one L-Proxy

Domain 2, 3 and 4 are connected to the same IP-852 (Ethernet/IP) channel and merged using an L-Proxy like shown in Figure 17.

7.3 Connecting more than 5 domains

By connecting several L-Proxy devices more than 5 domains can be merged (Figure 18). The first L-Proxy can connect 5 domains. All other L-Proxy devices can connect 4 domains. Every L-

Proxy needs to have one IP-852 node be configured in the same domain (domain 4 in Figure 18) to be able to exchange data.

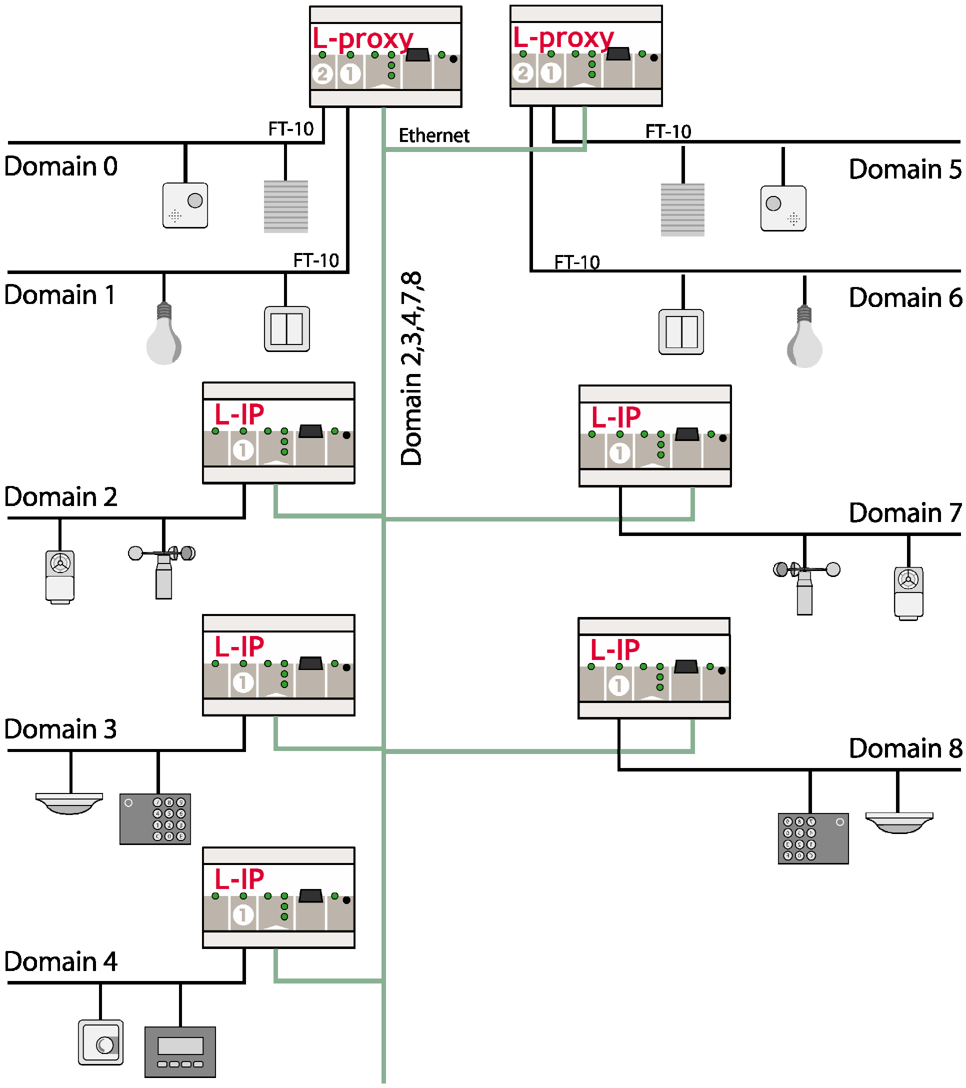


Figure 18: 2 L-Proxy to merge more than 5 domains

8 Remote Network Analysis and Maintenance

LOYTEC network infrastructure products have built in diagnostic features. Errors like channel overload or bad packets are reported by diagnostic LEDs. If the LED is flashing red a potential problem exists on the network segment connected to this port. This state is referred to as overload condition.

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70% or
- the collision rate was higher than 5% or
- more than 5% CRC on a port
- the L-IP was not able to process all available messages.

Statistics data about network traffic and errors are also logged in the devices. This information can be read from the devices over the network with the LOYTEC System Diagnostics Tool (LSD Tool). This tool gives a good overview about the health state of the entire network.

The network infrastructure devices can be read with the LSD Tool locally or remotely (Figure 19). The LSD Tool can find all LOYTEC network infrastructure products when connected locally (1,2), via remote IP-852 connections (3,4) or with a NIC709-IP interface (5).

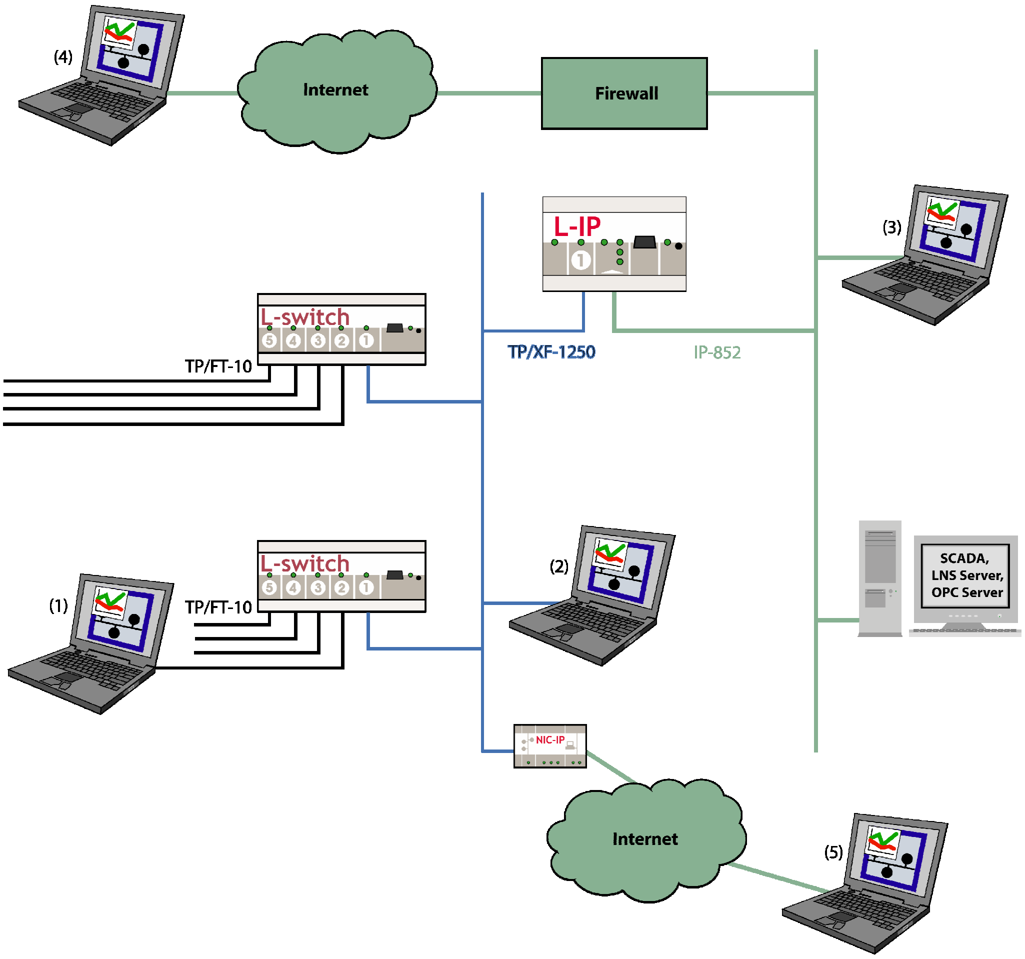


Figure 19: Local and remote access with the LSD tool.

However, in order to find the reason for network errors this requires a detailed analysis of the network traffic. This analysis can be done with the LPA protocol analyzer. The protocol analyzer listens to the network traffic and displays the recorded data on an intuitive Windows user interface.

The protocol analyzer can only record the packets on the channel to which it is currently connected. To provide the possibility to analyze the network traffic on remote channels, the L-IP devices have a built-in interface for the LPA-IP protocol analyzer software. The LPA-IP allows selecting any of the L-IP devices over an Ethernet connection and monitors the traffic of the network segment, which is connected to the L-IP device.

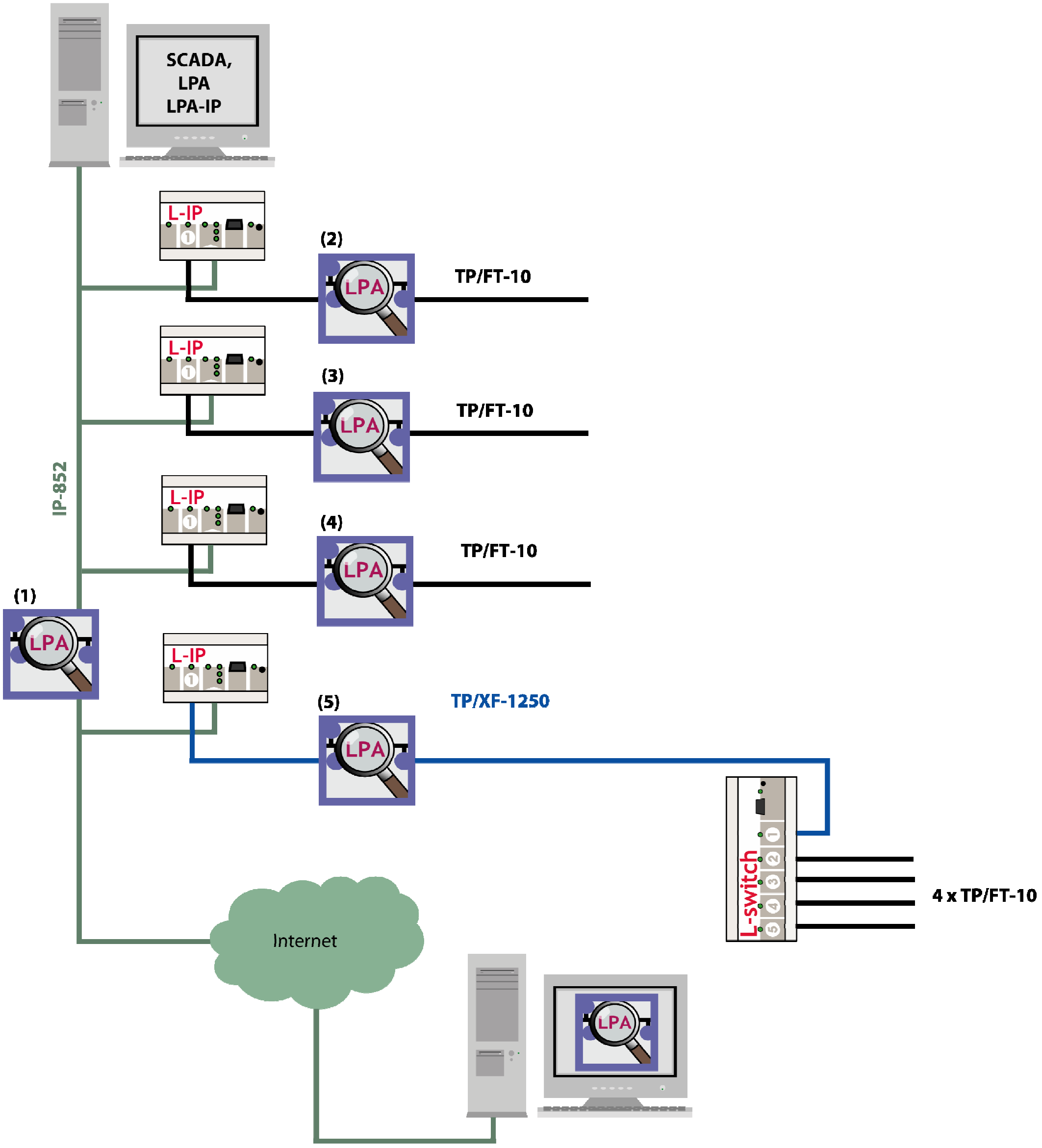


Figure 20: Remote network analysis with the LPA and LPA-IPs.

Figure 20 shows the different possibilities for a remote network analysis. The LPA-IP can monitor the network traffic on the IP-852 channel (1) as well as the remote traffic behind the L-IP devices (2, 3, 4, and 5).

Network segments which are not connected to an L-IP, a NIC-IP can be installed in the network and remotely accessed by the LPA software over an IP connection. Of course it is also possible to use a local network interface (e.g. NIC-USB) for local network analysis (see Figure 21).

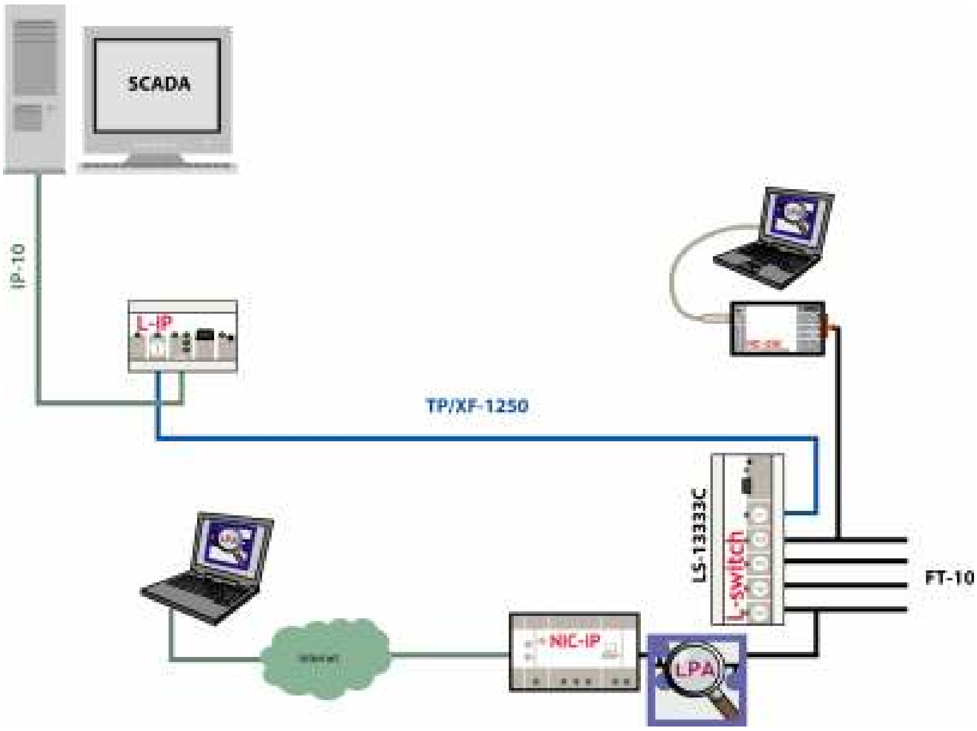


Figure 21: Remote access over NIC709-IP and local access using a NIC709-USB.

9 Remote Network Access over ISDN Lines

For many applications it is desirable to access the application site remotely without having a permanent internet connection to the site. In that case, the IP connection to a remote site can be established using an ISDN connection. The remote access can be established with a remote network interface like the NIC709-IP (see Figure 22) or in a way that the IP-852 channel is extended over the ISDN connection (see Figure 23). The second approach has the advantage that the remote LPA protocol analyzer functionality (see section 8) can also be used over the ISDN line.

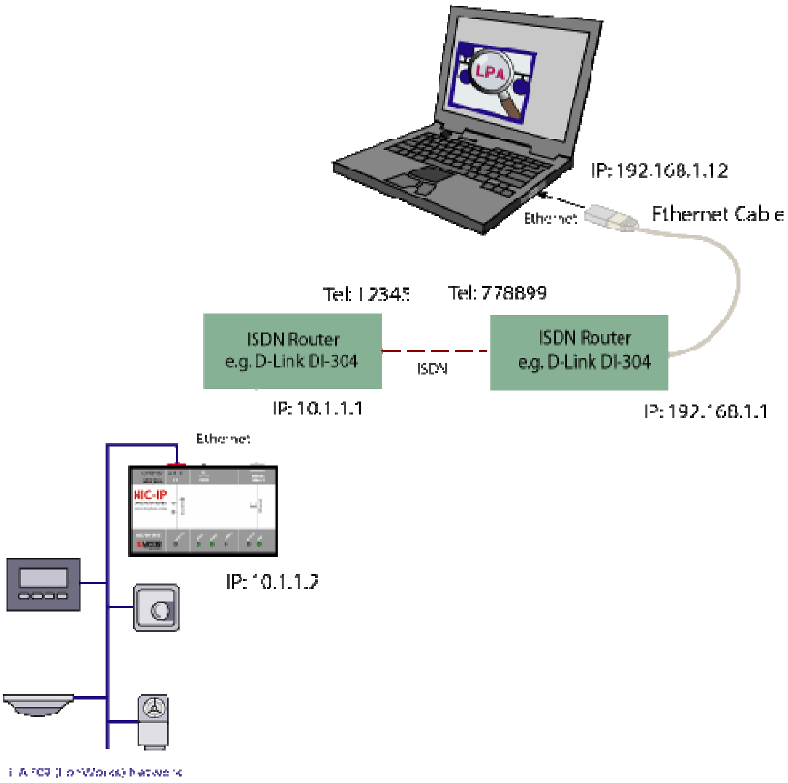


Figure 22: Remote connection over ISDN line using a NIC709-IP.

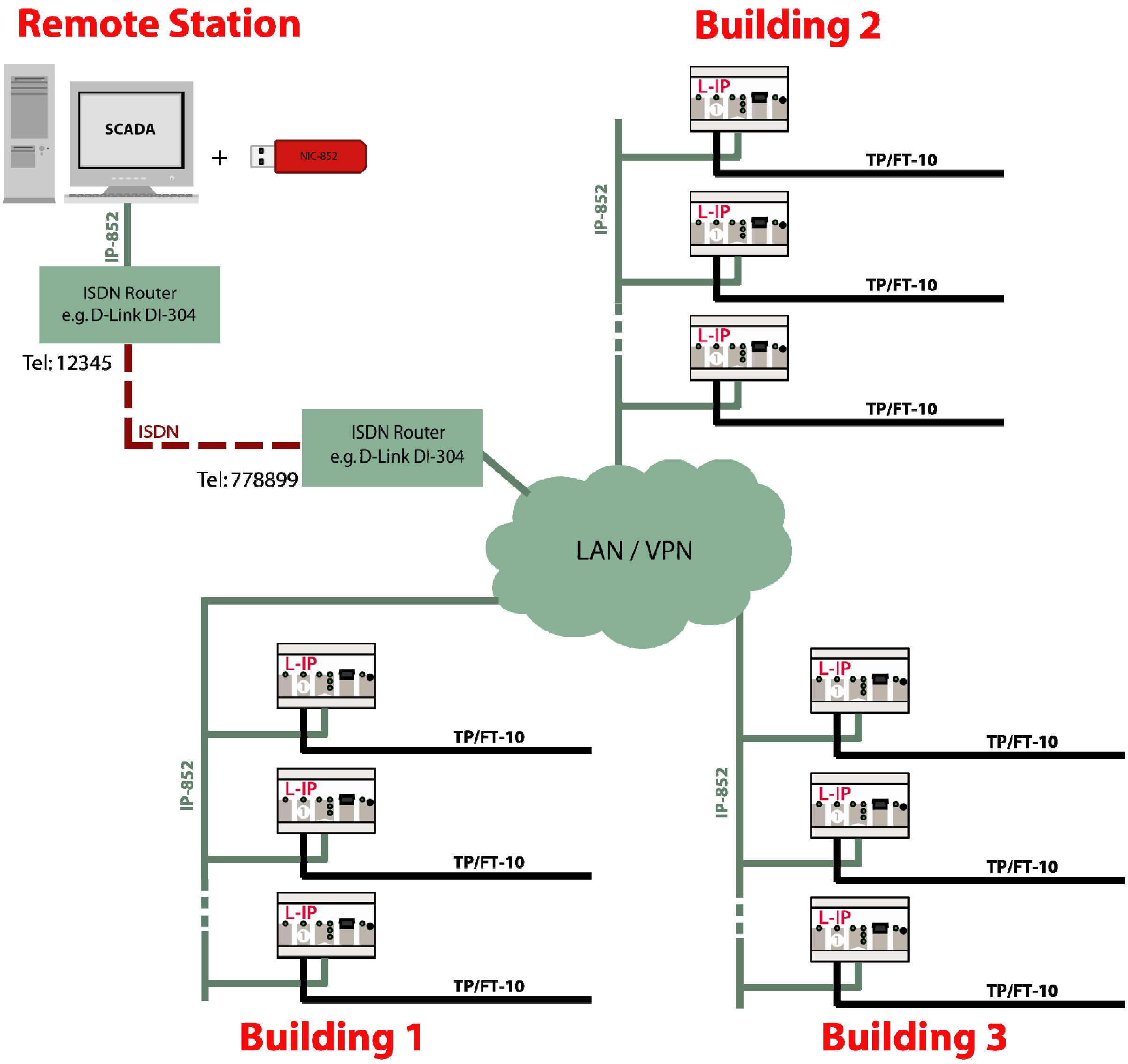


Figure 23: Remote extension of an IP-852 channel using an ISDN line.

Remote access over ISDN lines can be established in two ways:

1. Transparent LAN-to-LAN connection with dial on demand access
2. Dial-In access to a remote network.

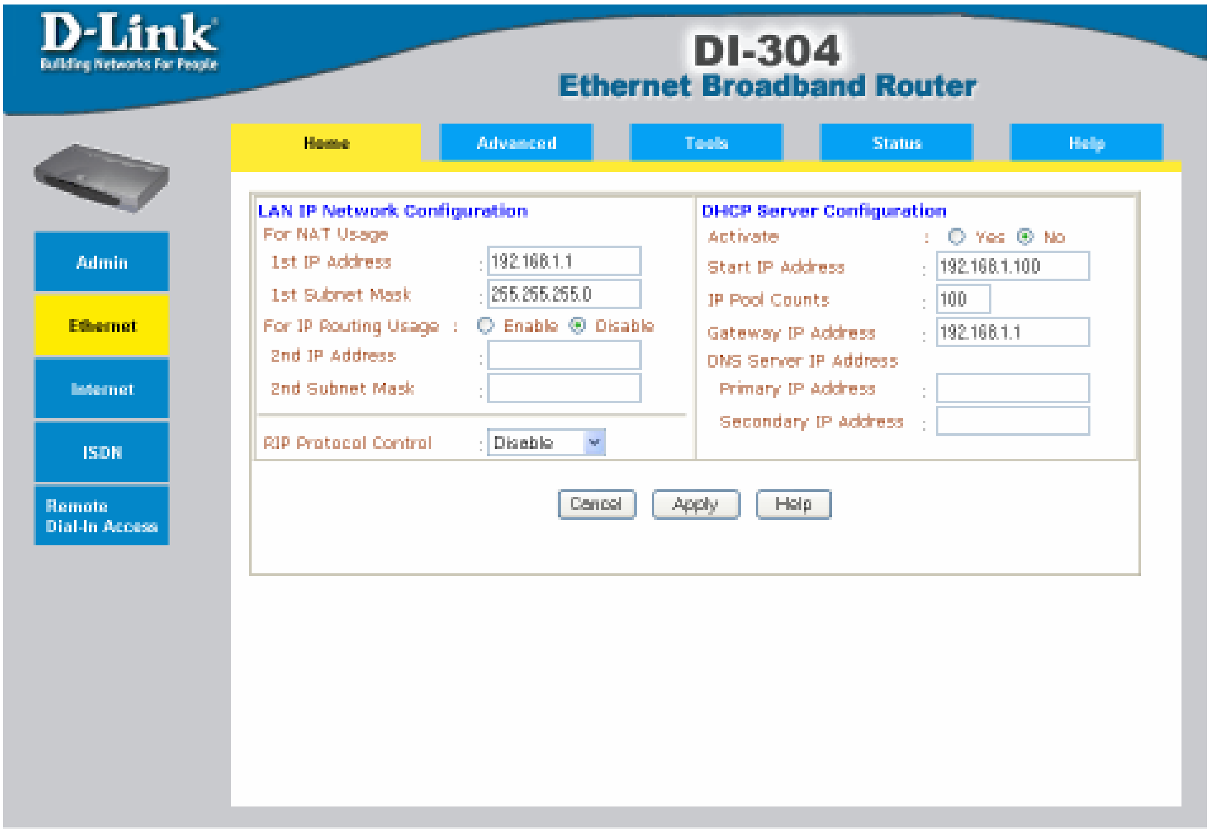
Different computer hardware vendors offer embedded router devices which provide functions for both, LAN-to-LAN connection and dial in support. An example configuration using the D-Link DI-304 router is described in the following chapters.

9.1 LAN-to-LAN connection

In this LAN-to-LAN connection example, the setup in Figure 22 is implemented. The PC is connected to one of the local Ethernet ports of the ISDN Router. It is not necessary to make a direct connection between the PC and the Router, but both devices must be members of the same Ethernet network. The ISDN Router is configured to automatically dial up a second ISDN Router whenever a device in the remote Ethernet network is contacted. Together with the second ISDN Router, a transparent Ethernet connection is established. After a configurable idle time, the ISDN connection is terminated.

The D-Link ISDN Router has a built in web server which allows to configure the settings of the device. A step-by-step description of the router configuration for the LAN-to-LAN scenario follows.

1. First the local IP settings have to be established (see Figure 24). In the example, the local ISDN router has assigned the IP address 192.168.1.1. It also provides a DHCP server which assigns addresses in the IP range starting with 192.168.1.100.

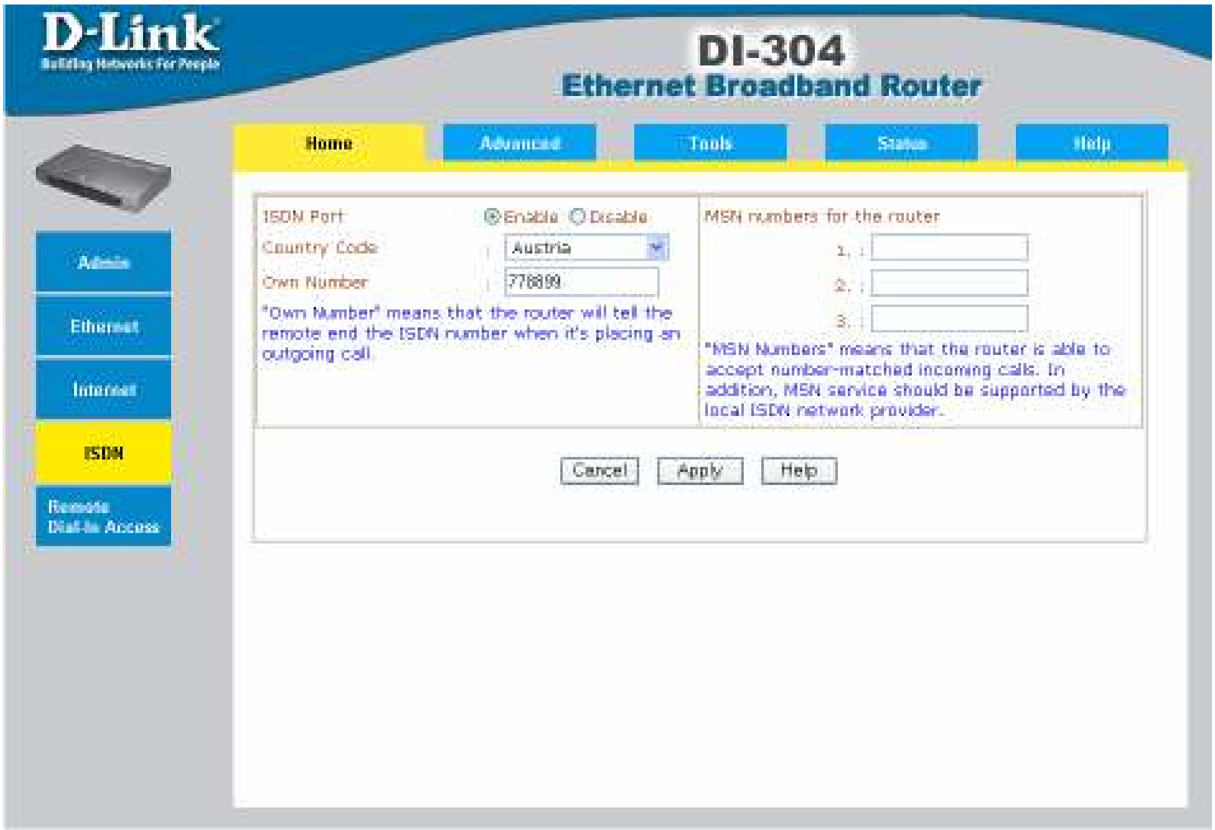


LAN IP Network Configuration
For NAT Usage
1st IP Address : 192.168.1.1
1st Subnet Mask : 255.255.255.0
For IP Routing Usage : ○ Enable ● Disable
2nd IP Address :
2nd Subnet Mask :
RIP Protocol Control : Disable

DHCP Server Configuration
Activate : ○ Yes ● No
Start IP Address : 192.168.1.100
IP Pool Counts : 100
Gateway IP Address : 192.168.1.1
DNS Server IP Address
Primary IP Address :
Secondary IP Address :

Figure 24: Ethernet configuration of ISDN Router 1

2. The second step is to configure the local ISDN settings (see Figure 25). The ISDN port is enabled and the own telephone number has to be entered.



ISDN Port ● Enable ○ Disable

Country Code : Austria

Own Number : 778899

"Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.

MSN numbers for the router

1. :

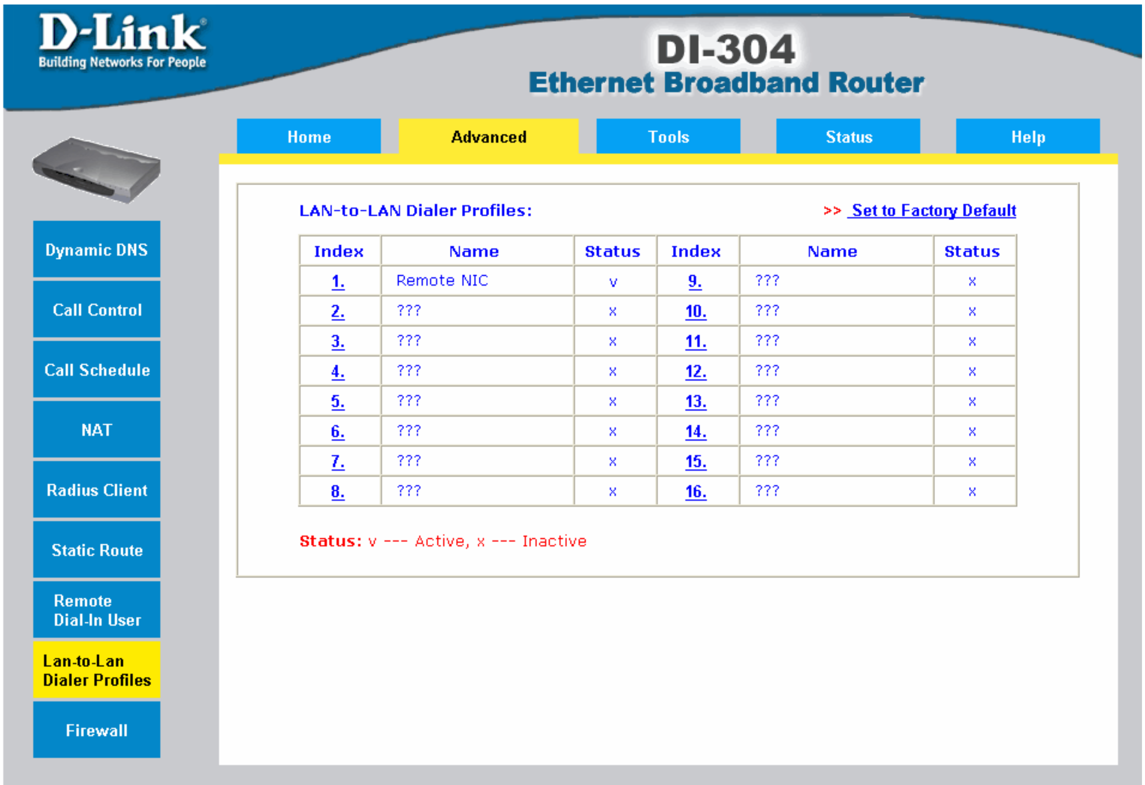
2. :

3. :

"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.

Figure 25: ISDN Configuration of ISDN Router 1

3. To provide automatic dial in functionality, a LAN-to-LAN dialer profile has to be configured (see Figure 26, Figure 27, Figure 28). The first step is to create a new LAN-to-LAN profile. In the next configuration screen, the profile has to be enabled. Additional configuration is needed for the remote telephone number to dial and a user name and password for the access of the remote ISDN router. To allow automatic termination of ISDN link, an idle timeout can be set. If required, additional settings like the Link Type can be made.

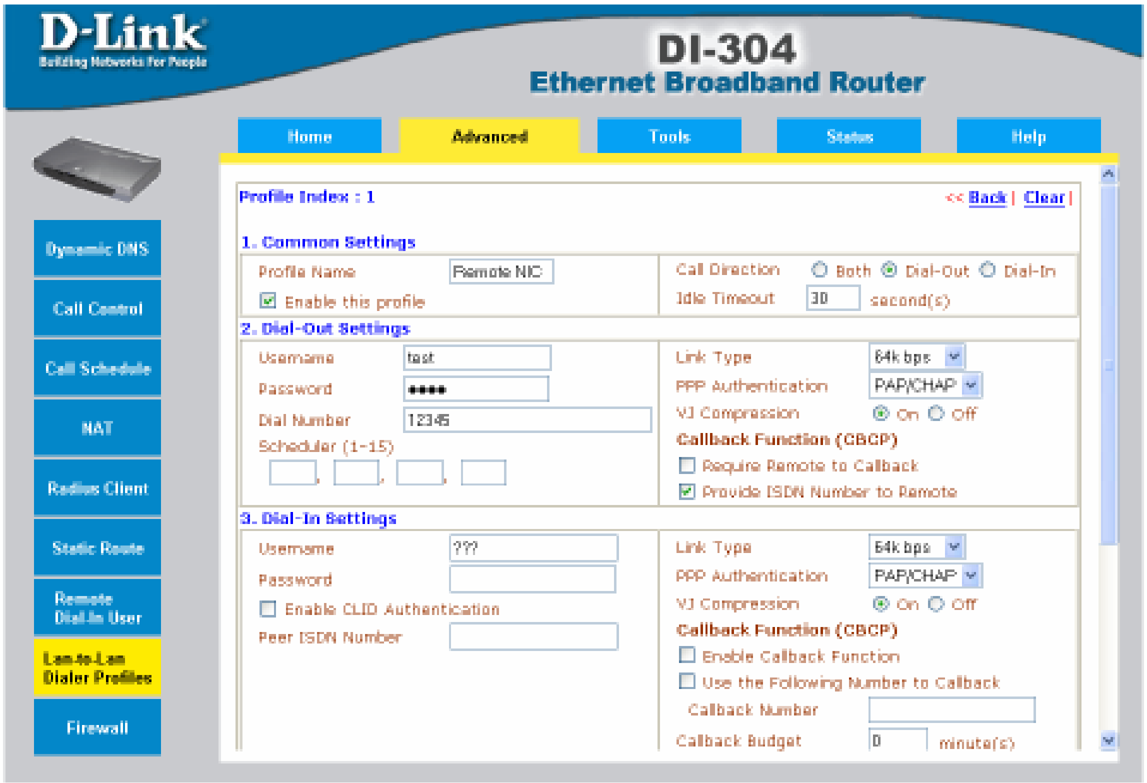


LAN-to-LAN Dialer Profiles:

Index	Name	Status	Index	Name	Status
1.	Remote NIC	v	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

Status: v --- Active, x --- Inactive

Figure 26: Enabling Lan-to-Lan Dialer Profiles



Profile Index : 1

1. Common Settings

Profile Name: Remote NIC

☑ Enable this profile

Call Direction: ○ Both ● Dial-Out ○ Dial-In

Idle Timeout: 30 second(s)

2. Dial-Out Settings

Username: test

Password: ****

Dial Number: 12345

Scheduler (1-15): , , ,

Link Type: 64k bps

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

Callback Function (CBCP)

□ Require Remote to Callback

☑ Provide ISDN Number to Remote

3. Dial-In Settings

Username: ???

Password:

□ Enable CLID Authentication

Peer ISDN Number:

Link Type: 64k bps

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

Callback Function (CBCP)

□ Enable Callback Function

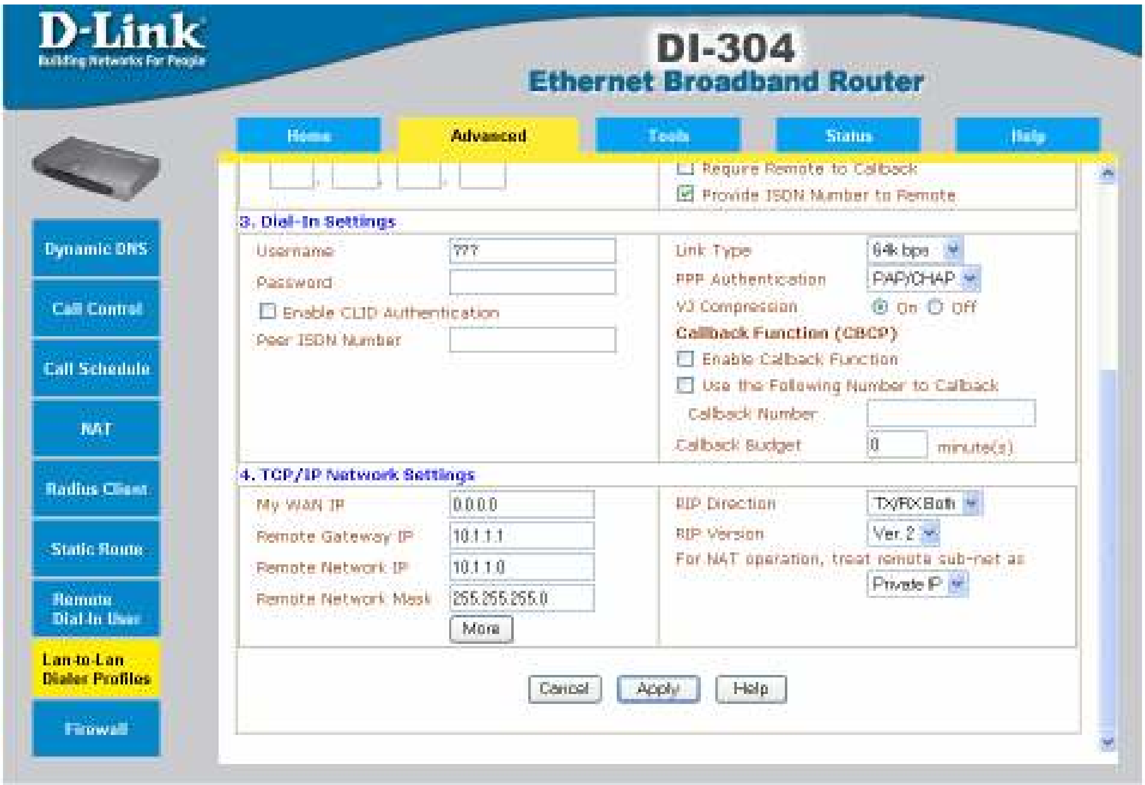
□ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

Figure 27: LAN-to-LAN Profile of ISDN Router 1 (1)

4. For automatic dial in support, the IP address range of the remote network must be configured (see Figure 28). The remote Gateway IP and remote network IP are required. It is possible to define multiple LAN-to-LAN profiles and connect multiple remote IP networks. In that case, the remote network IP ranges have to be different in order to allow correct routing and dial in access to the remote networks.



□ Require Remote to Callback
☑ Provide ISDN Number to Remote

3. Dial-In Settings

Username: ???
Password:
□ Enable CLID Authentication
Peer ISDN Number:

Link Type: 64k bps
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off
Callback Function (CBCP)
□ Enable Callback Function
□ Use the Following Number to Callback
Callback Number:
Callback Budget: 0 minute(s)

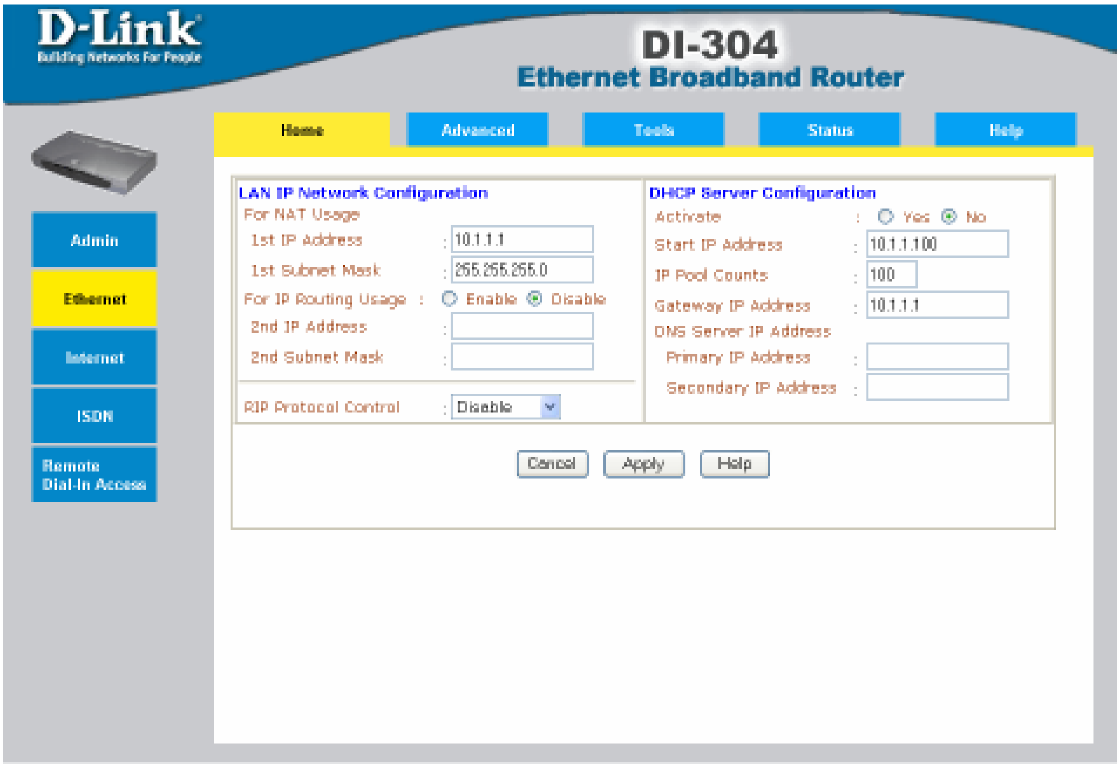
4. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 10.1.1.1
Remote Network IP: 10.1.1.0
Remote Network Mask: 255.255.255.0

RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP

Figure 28: LAN-to-LAN Profile of ISDN Router 1 (2)

5. The IP and ISDN configuration of the remote router device is shown in Figure 29 and Figure 30.



LAN IP Network Configuration

For NAT Usage

1st IP Address : 10.1.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage : ○ Enable ● Disable

2nd IP Address :

2nd Subnet Mask :

RIP Protocol Control : Disable

DHCP Server Configuration

Activate : ○ Yes ● No

Start IP Address : 10.1.1.100

IP Pool Counts : 100

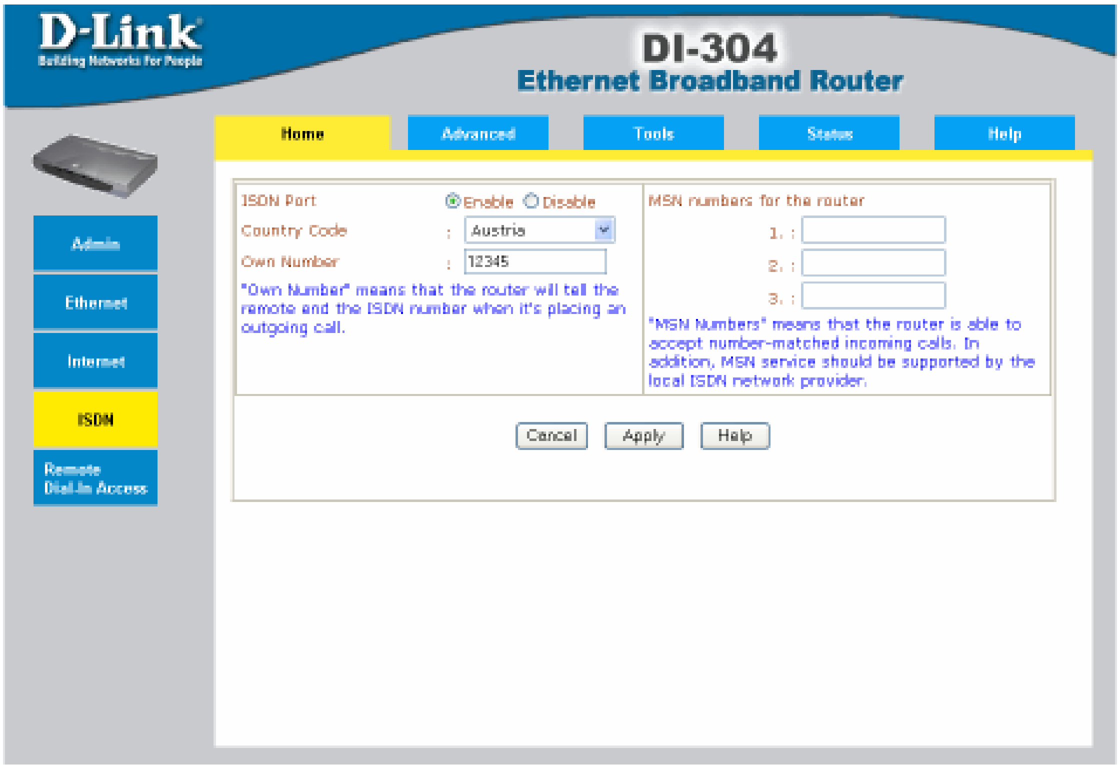
Gateway IP Address : 10.1.1.1

DNS Server IP Address

Primary IP Address :

Secondary IP Address :

Figure 29: Ethernet configuration of ISDN Router 2



ISDN Port ● Enable ○ Disable

Country Code : Austria

Own Number : 12345

"Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.

MSN numbers for the router

1. :

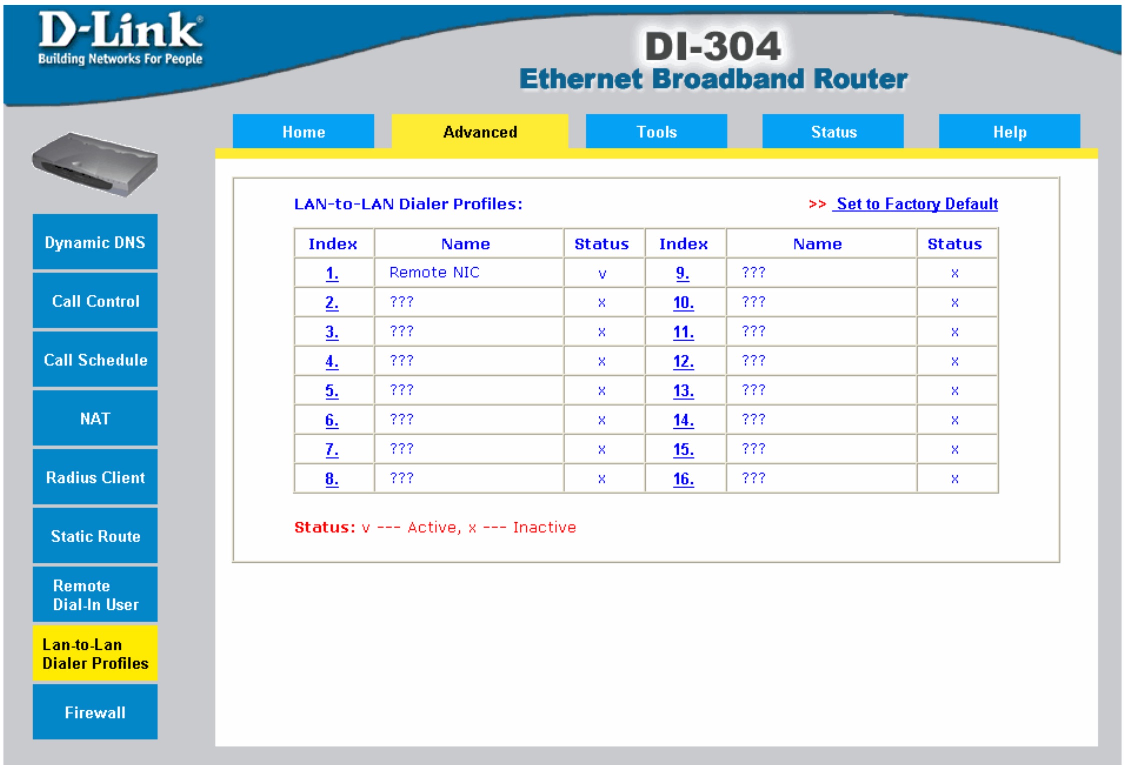
2. :

3. :

"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.

Figure 30: ISDN Configuration of ISDN Router 2

6. Also in this router a LAN-to-LAN profile is created (Figure 31).



LAN-to-LAN Dialer Profiles:

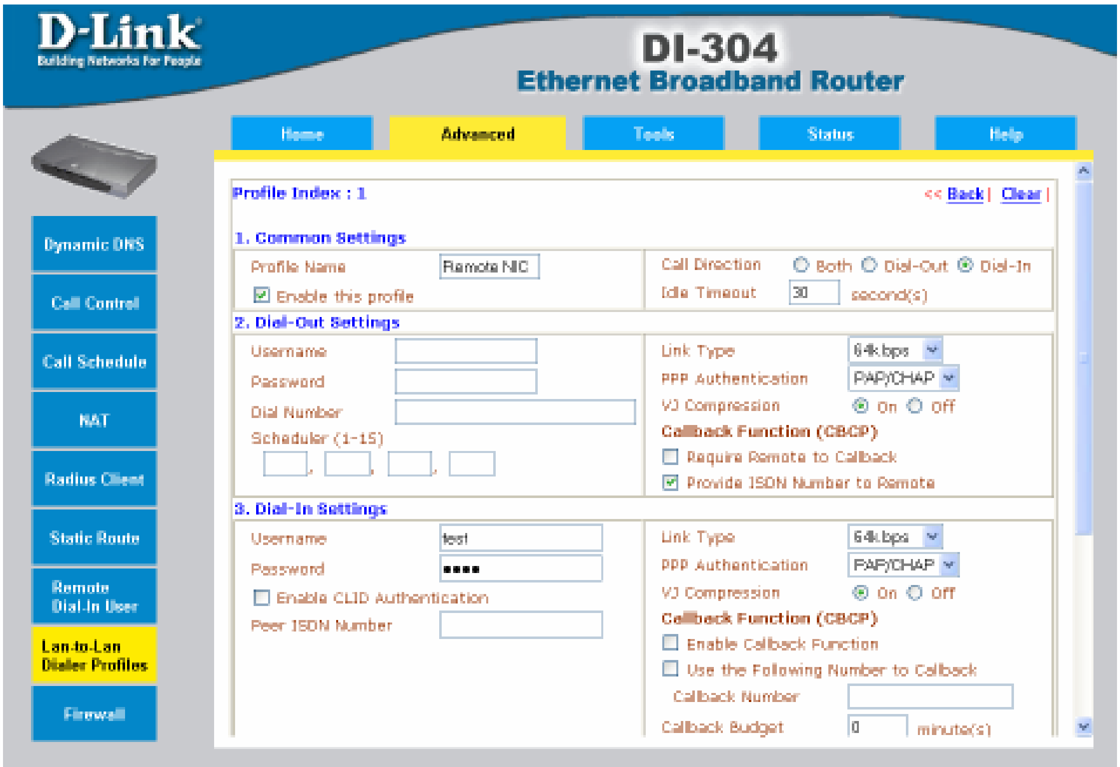
>> Set to Factory Default

Index	Name	Status	Index	Name	Status
1.	Remote NIC	v	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

Status: v --- Active, x --- Inactive

Figure 31: Enabling Lan-to-Lan Dialer Profiles in Router 2

7. The user name and password settings have to match the settings adjusted in the LAN-to-LAN profile of the local router (Figure 32).



Profile Index : 1

<< Back | Clear |

1. Common Settings

Profile Name: Remote NIC

☑ Enable this profile

Call Direction: ○ Both ○ Dial-Out ● Dial-In

Idle Timeout: 30 second(s)

2. Dial-Out Settings

Username:

Password:

Dial Number:

Scheduler (1-15): , , ,

Link Type: 64k bps

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

Callback Function (CBCP)

□ Require Remote to Callback

☑ Provide ISDN Number to Remote

3. Dial-In Settings

Username: test

Password: ****

□ Enable CLID Authentication

Peer ISDN Number:

Link Type: 64k bps

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

Callback Function (CBCP)

□ Enable Callback Function

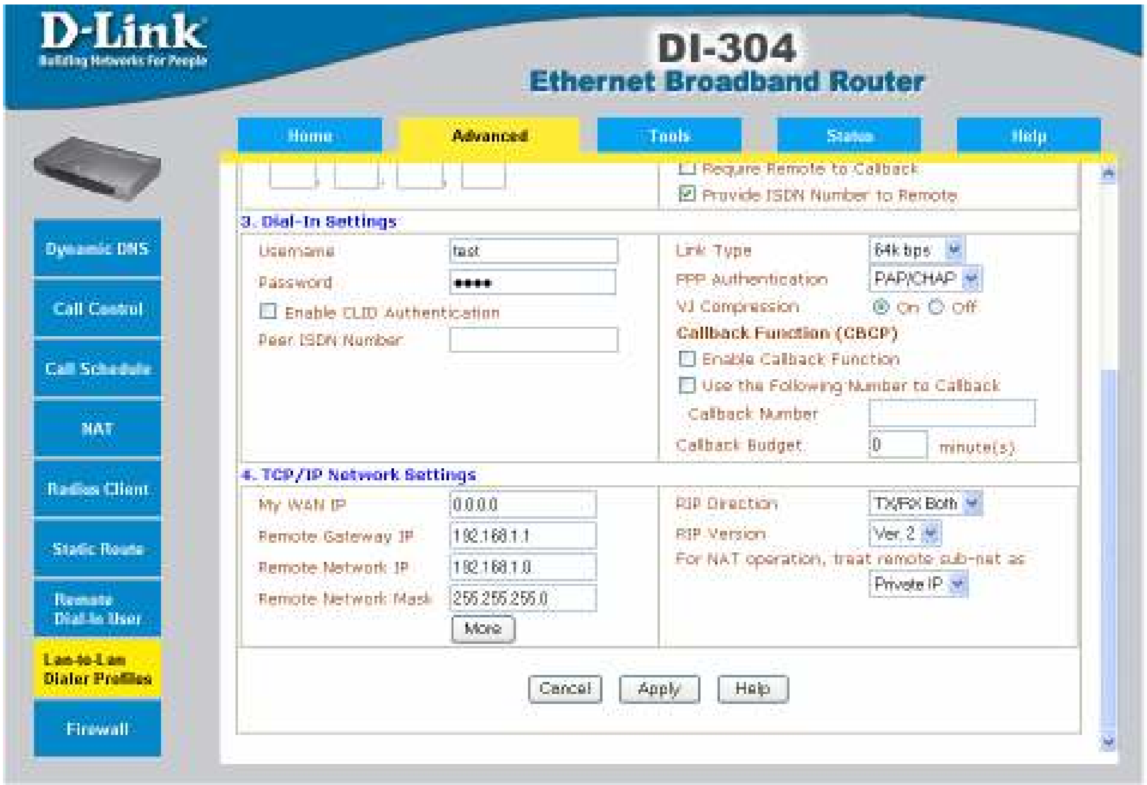
□ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

Figure 32: LAN-to-LAN Profile of ISDN Router 2 (1)

8. Finally, the IP setting have to match the IP address range of the local network, in order to allow correct routing and dial-in support. (Figure 33).



□ Require Remote to Callback
☑ Provide ISDN Number to Remote

3. Dial-In Settings

Username: test
Password: ●●●●
□ Enable CLID Authentication
Peer ISDN Number:

Link Type: 64k bps
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off
Callback Function (CBCP)
□ Enable Callback Function
□ Use the Following Number to Callback
Callback Number:
Callback Budget: 0 minute(s)

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0
Remote Gateway IP: 192.168.1.1
Remote Network IP: 192.168.1.0
Remote Network Mask: 255.255.255.0

RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP

Figure 33: LAN-to-LAN Profile of ISDN Router 2 (2)

With the described configuration, the ISDN routers would automatically dial into the remote network whenever a device on the local network accesses an IP address which is located in the remote network. This e.g. would be the case when a configuration tool opens a NIC709-IP device which has defined an IP address of the remote IP network.

9.2 Dial-In Access

Just like the described configuration, it is also possible to provide dial-in access to a remote network. The configuration process is similar to the configuration described in the previous section. Instead of using two ISDN routers, Dial-In access would require only one router on the remote network. Instead of the local ISDN router, an ISDN adapter card would be used on the local PC. Different to the described solution, the connection would have to be established manually in most cases.

10 Glossary

This section defines the terms used in throughout this document:

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

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

- A **Port** is a connection to a network channel. Network infrastructure products have multiple ports so that multiple channels can be connected. Application nodes typically have only one port.

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

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

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

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

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

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

- **Channel types**:

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

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

  - **Collision-less TP/XF-1250**: A high speed channel, which uses the TP/XF-1250 transceiver but uses a collision-less high speed bus arbitration protocol.

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

  - **TP-RS485-xxx**: A channel which uses a TP-RS485 transceiver. Xxx defines different bit rates, e.g. TP-RS485-39 or TP-RS485-78 for 39kbit and 78 kbit channels.

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

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

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

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

- The **Configuration Server** is administrating the relation between the EIA-709-1 addresses (domain, subnet, node, router typ, …) and the IP addresses on the IP-852 channel. Only one configuration server can be active on an IP-852 channel. One Server can manage several domains.

11 References

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

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

[3] LOYTEC electronics GmbH: Application Note AN006E L-Switch and LNS, Document Number 86001004

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

[5] LonMark Deutschland e.V..: LonWorks Installation Handbook, VDE Verlag GmbH, 2002

[6] L-IP Benutzerhandbuch, LOYTEC electronics GmbH, Version 4.5, Document Number 88065909.

[7] LOYTEC electronics GmbH: Application Note AN008E, Network Troubleshooting White Paper, Document Number 86001401

12 Legal notice

LPA, L-Chip, L-Switch, L-IP, L-Proxy, L-OPC, L-DALI, L-Gate, L-Core, LC3020 are trademarks of LOYTEC electronics GmbH. Echelon, LON, LONWORKS, i.LON, LNS, LonMaker, and Neuron are trademarks of Echelon Corporation registered in the United States and other countries. LONMARK and the LONMARK Logo are managed, granted, and used by LONMARK International under a license granted by Echelon Corporation. Other trademarks and trade names used in this document refer either to the entities claiming the markets and names, or to their products. LOYTEC disclaims proprietary interest in the markets and names of others. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of LOYTEC. Product specifications, availability, and design are subject to change without prior notice.

13 Revision History

Date	Version	Author	Description
30.04.2004	1	NR	Initial Version
17.06.2005	2	NR	Added chapter about remote ISDN connections Added L-IP 33ECTB
		NR	Removed 6 domain limit on L-IP configuration server (not valid any more)
2006-12-04	3	NR	Colissionless Backbone Modus deleted L-IP 3333ECTB added Explanation to L-IP und NAT Router added Explanation to NIC-852 added Explanation of L-Proxy adapted toLP-33E100.
2007-01-18		DAD	Graphis adapted to new hardware. Added the „B“ in graphis with L-Switch. Table 2: Colissionless Backbone deleted. Chapter 8: "Meaning" of the red LED added. Chapter 8: moved LSD-Tool before LPA-Tool - Referenz: [1] LonMark Interoperability Association: LonMark Layer

			1-6 Interoperability Guidelines, Version 3.4, September 2005 (Current version) - Referenz: [3] LOYTEC electronics GmbH: Application Note AN008E, Network Troubleshooting White Paper, Document Number 86001401 (Current version)