

ELSA LANCOM™ VPN Option

© 2001 ELSA AG, Aachen (Germany)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. ELSA shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from ELSA. We reserve the right to make any alterations that arise as the result of technical development.

ELSA is DIN EN ISO 9001 certified. The accredited TÜV CERT certification authority has confirmed ELSA conformity to the worldwide ISO 9001 standard in certificate number 09 100 5069, issued on June 15, 1998.

You can find all declarations and approvals for the products, as long as they were available at the time of publication, in the appendix of this documentation.

Trademarks

Windows®, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

Cisco is a registered trademark of Cisco Systems, Inc.

SSH Secure Shell, SSH IPSEC Express, SSH NAT Traversal, SSH Sentinel and SSH Certifier are trademarks of SSH Communications Security.

ELSA LANCOM VPN products are manufactured under license from SSH Communications Security. The following applies for all product components from SSH: © 2000 SSH Communications Security. All rights reserved.

The ELSA logo is a registered trademark of ELSA AG. All other names mentioned may be trademarks or registered trademarks of their respective owners.

Subject to change without notice. No liability for technical errors or omissions.

ELSA AG
Sonnenweg 11
52070 Aachen
Germany

www.elsa.com

Aachen, July 2001

Preface

Thank you for placing your trust in this ELSA product.

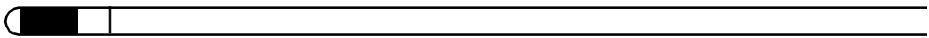
With *LANCOM VPN Option*, you can enable your *ELSA LANCOM* to set up so-called virtual private networks. You can then establish cost-effective network links via the Internet without sacrificing the customary high data security associated with direct connections.

One special feature of *LANCOM VPN* is *LANCOM Dynamic VPN*; ELSA has applied for a patent for this technology. While VPNs normally require static IP addresses, the *LANCOM Dynamic VPN* also permits VPN connections using dynamic IP addresses. You can thus use the *LANCOM VPN* with any Internet connection.

This documentation was compiled by several members of our staff from a variety of departments in order to ensure you the best possible support when using your ELSA product.

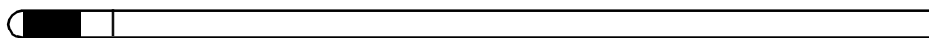


Our online services (www.elsa.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the Support file section under 'Know-how', you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.



Contents

1 Introduction	7
1.1 Package contents of the <i>ELSA LANCOM VPN Option</i>	7
1.2 What are the advantages of VPN?	7
1.2.1 Private IP addresses on the Internet?	10
1.2.2 Secure communications via the Internet?	10
1.2.3 VPN for Internet connections only?	12
1.3 VPN connections in detail	12
1.3.1 LAN-LAN coupling.	12
1.3.2 Dial-up connections (Remote Access Service)	13
1.4 What is <i>ELSA LANCOM Dynamic VPN</i> ?	14
1.4.1 A look at IP addressing	14
1.4.2 This is how <i>ELSA LANCOM Dynamic VPN</i> works.	16
1.5 An overview of <i>ELSA LANCOM VPN</i>	18
1.6 What now?	19
2 Installation of the VPN option	21
2.1 Installation requirements	21
2.1.1 Supported <i>ELSA LANCOM</i>	21
2.1.2 Package contents	21
2.1.3 Access to the device and <i>ELSA LANconfig</i> .	22
2.1.4 Checking the <i>ELSA LANconfig</i> version	22
2.1.5 Checking the firmware version	22
2.1.6 Updating the firmware	23
2.2 Online registration	24
2.3 Activating the VPN option	25
2.4 Checking the activation	26
3 Setting up the VPN connection	27
3.1 The <i>ELSA LANconfig</i> Wizard for VPN	27
3.2 What will the wizard ask?	28
3.2.1 Overview of configuration entries	28
3.2.2 Meaning of the configuration entries	30
3.3 Examples of VPN configurations	35
3.3.1 VPN via direct connection	35
3.3.2 VPN via the Internet	37



3.4	Setting up the basic connection	40
3.4.1	Direct connections	40
3.4.2	Connections via the Internet	40
3.5	Before entering the VPN connection data	41
3.6	Entering the data and testing the VPN connection	41

4 The technology behind VPN **43**

4.1	How does VPN work?	43
4.1.1	IPSec—the foundation of <i>ELSA LANCOM VPN</i>	43
4.1.2	Alternatives to IPSec	44
4.2	The standards behind IPSec	46
4.2.1	IPSec modules and their tasks	46
4.2.2	Security associations—numbered tunnels	46
4.2.3	Authentication—the AH protocol	47
4.2.4	Encryption of the packets—the ESP protocol	50
4.2.5	Key management—IKE	52

1 Introduction

This chapter provides answers to the three following questions:

- What is included in the package contents of the *ELSA LANCOM VPN Option*?
- What are the advantages of VPN?
- What are the capabilities and properties of the *ELSA LANCOM VPN*?

1.1 Package contents of the *ELSA LANCOM VPN Option*

First, please check that the *ELSA LANCOM VPN Option* package also contains the following components in addition to this manual:

- *ELSA LANCOM VPN Option* CD
- Proof of license (yellow sticker)

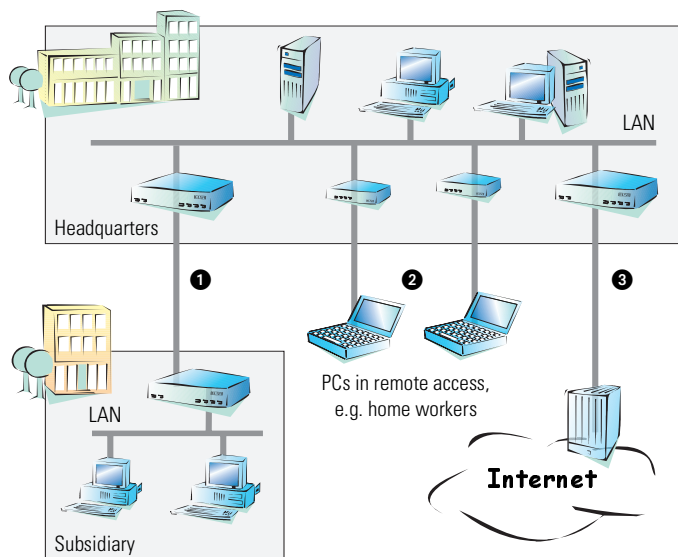
1.2 What are the advantages of VPN?

A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up cost-effective, public IP networks, for example via the ultimate network: the Internet.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:



The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

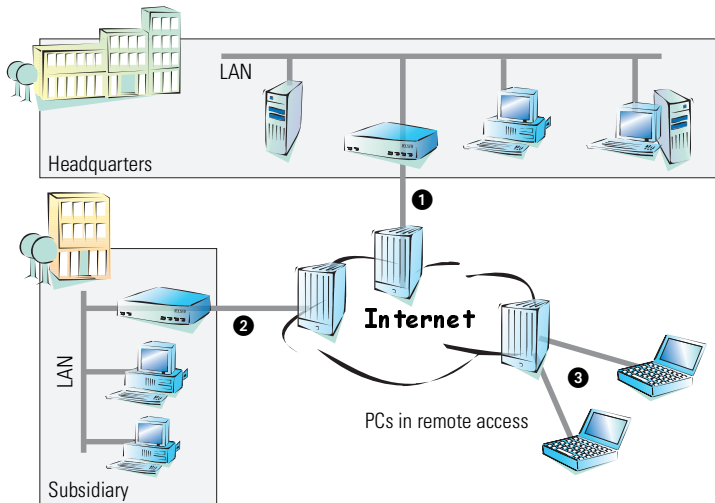
- ❶ A subsidiary is connected to the LAN, typically using a leased line.
- ❷ PCs dial into the central network via modem or ISDN connections (remote access—RAS).
- ❸ The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection (analog dial-up, ISDN, leased lines). In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

Networking via the Internet

The following structure results when using the Internet (or other IP-based public networks) instead of direct connections:



All participants have fixed or dial-up connections to the Internet. Expensive dedicated lines are no longer needed.

- ❶ All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.
- ❷ The subsidiary also has its own connection to the Internet.
- ❸ The RAS PCs connect to the headquarters LAN via the Internet.

The Internet is available virtually everywhere and typically has low access costs. Significant savings can thus be achieved in relation to switched or dedicated connections, especially over long distances.

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: it can be a conventional ISDN line. Broadband technologies such as DSL, cable modems or 2-Mbit leased lines can also be used.

The technologies of the individual participants do not have to be compatible to one another, as would be the case for conventional direct connections. A

single Internet access can be used to establish multiple simultaneous logical connections to a variety of remote stations.

The resulting savings and high flexibility makes the Internet (or any other IP network) an outstanding backbone for a corporate network.

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- The necessity of public IP addresses for Internet users
- The lack of data security of unprotected data transfers

1.2.1

Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. Other computers with public IP addresses can only communicate via the Internet with such routers. PCs in the LAN with private addresses can not be addressed from the Internet.

Routing at the IP level with VPN

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

VPN handles the conversion between private and public IP addresses. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

1.2.2

Secure communications via the Internet?

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the

Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

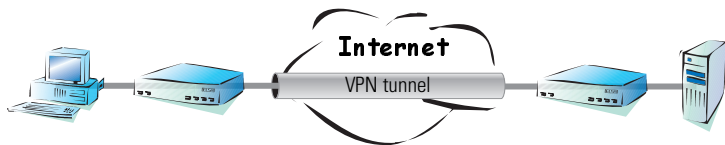
VPN—Security through encryption

VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties. The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as “keys” are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain “private”, inaccessible to unauthorized parties.

Send your data through the tunnel—for security's sake

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as “tunnels”.



The goal of modern network structures has thus been achieved: secure connections via low-cost IP networks. It's all possible thanks to tunnels.

1.2.3

VPN for Internet connections only?

The VPN concept was designed especially for the realization of virtual network structures via public IP networks, especially the Internet.

Security considerations are not only relevant to the Internet. It is also possible to monitor and manipulate data sent via private, closed networks for direct connections such as the telephone network or ISDN. The actual extent of this misuse is very controversial. The existence of a risk is almost universally acknowledged, however.

Reason enough to provide additional security for communication via dedicated lines as well. VPN is also suitable as a security concept for network structures based on actual dedicated lines.

ELSA LANCOM VPN can be used for both the Internet and dedicated connections. ISDN dial-up connections, leased ISDN lines and 2-Mbit leased lines are supported.



To maintain a clear overview, all of the following explanations and examples will use the Internet as the basis for VPNs. The Internet is representative for other connection options. Private IP networks or direct connections can therefore always be used in place of the Internet.

1.3

VPN connections in detail

Two types of VPN connections are available:

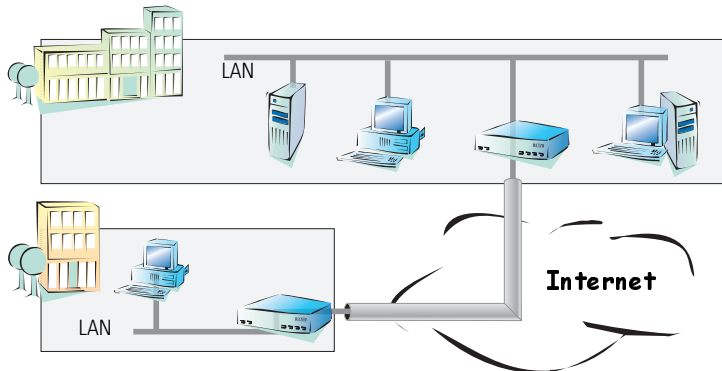
- VPN connections linking two local networks. This type of connection is also known as a “LAN-LAN coupling”.
- The connection of an individual computer with a network, generally via a dial-up connection (RAS).

1.3.1

LAN-LAN coupling

The coupling of two remote networks is known as a LAN-LAN coupling. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN couplings are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

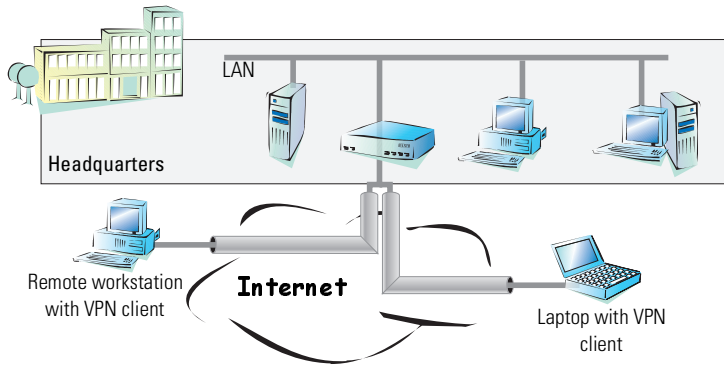
The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

1.3.2

Dial-up connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC. *ELSA LANCOM VPN* currently does not support dial-up connections using VPN client software. Only LAN-LAN couplings between two VPN gateways are possible. Support for VPN client software is currently in preparation.

For security reasons we recommend that you also always connect individual PCs via their own *ELSA LANCOM*.

1.4 What is *ELSA LANCOM Dynamic VPN*?

ELSA LANCOM Dynamic VPN is a patent-pending *ELSA* technology which permits VPN tunnels to be set up to remote stations that do not have a static, but only a dynamic IP address. *ELSA LANCOM Dynamic VPN* is a standard component of the *ELSA LANCOM VPN Option*.

Who needs *ELSA LANCOM Dynamic VPN* and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of static IP addresses. The second step shows the solution thereof with *ELSA LANCOM Dynamic VPN*.

1.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address—a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest of the Internet and a private one by which the computer can be reached within the local network.

Static and dynamic IP addresses

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. Dynamic IP addresses are assigned to Internet users by their Internet service providers (ISPs) for the duration of the connection when they log in. The ISP therefore uses a random unused address out of his IP address pool. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.

Advantages and disadvantages of dynamic IP addresses

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance—they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a dynamic address, A cannot know that address and therefore cannot contact B.

The *ELSA LANCOM Dynamic VPN* offers the answer here.

1.4.2

This is how *ELSA LANCOM Dynamic VPN* works

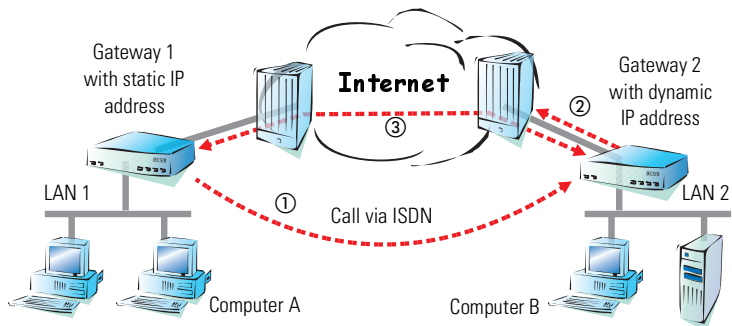
Let's use two examples to explain how *ELSA LANCOM Dynamic VPN* works (designations refer to the IP addressing type of the two VPN gateways):

- static – dynamic
- dynamic – dynamic

Static – dynamic

If the user of Computer A in LAN 1 would like to connect to Computer B in LAN 2, Gateway 1 will receive the request and will attempt to set up a VPN tunnel to Gateway 2. Gateway 2 only has a dynamic IP address and thus cannot be addressed directly via the Internet.

With *ELSA LANCOM Dynamic VPN*, the VPN tunnel can be set up nevertheless. The connection is established in three steps:



- ① Gateway 1 calls Gateway 2 via ISDN. It takes advantage of the ISDN functionality of sending its own subscriber number via the D-channel free of charge. Gateway 2 determines the IP address of Gateway 1 from the preconfigured VPN remote stations using the received subscriber number.

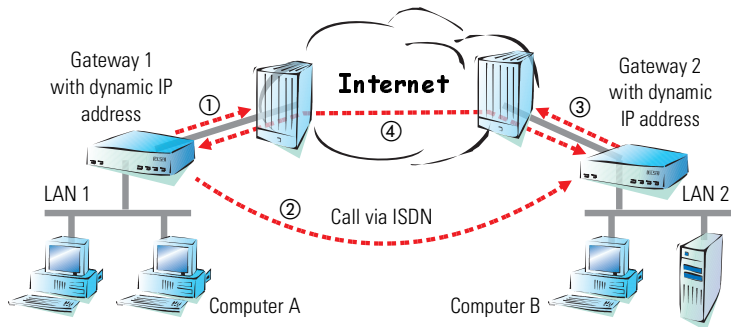
If Gateway 2 does not receive a subscriber number via the D-channel (if that particular ISDN service feature is not available, for example) or an unknown number is transferred, the authentication will be performed via the B-channel. Once the negotiation was successful, Gateway 1 sends its IP address and closes the connection on the B-channel immediately.

- ② Now it's Gateway 2's turn: It first connects to its ISP and is assigned a dynamic IP address.

- ③ Gateway 2 can now set up the VPN tunnel to Gateway 1. It already knows the static IP address of Gateway 1.

Dynamic – dynamic

With *ELSA LANCOM Dynamic VPN*, VPN tunnels can also be set up between two gateways that both only have dynamic IP addresses. Let's modify the previous example so that in this case Gateway 1 also has a dynamic IP address. Once again, Computer A would like to connect to Computer B:



- ① Gateway 1 connects to its ISP and is assigned a public, dynamic IP address.
- ② It then calls Gateway 2 via ISDN to send this dynamic address. Three procedures are used to send the address:
 - **As information in the LLC element of the D-channel.** In the D-channel protocol of Euro-ISDN (DSS-1), the so-called LLC (**L**ower **L**ayer **C**ompatibility) element can be used to send additional information to the remote station. This transfer takes place before the B-channel connection is established. Once the address has been sent successfully, the remote station rejects the call. Charges are thus not incurred for a B-channel connection. The IP address is sent nevertheless—for free in this case.



The LLC element is generally available as a standard feature in Euro-ISDN that does not require registration or activation. It may be disabled by telephone companies or individual exchanges, however. The LLC element is not available in 1TR6, the German national ISDN. The procedure described above thus will not work with 1TR6.

- **As a subaddress via the D-channel.** If it is not possible to send the address via the LLC element, Gateway 1 will attempt to send the address as a so-called subaddress. Like the LLC element, the subaddress is an information element of the D-channel protocol that permits short items of information to be sent free of charge. In this case, the telephone company must enable the 'subaddressing' feature first; this is generally subject to a charge. As with the LLC element, the call is rejected by the remote station once the IP address has been transferred successfully. The connection thus remains free of charge.
 - **Via the B-channel.** If both attempts to send the IP address via the D-channel fail, then a conventional connection via the B-channel must be established to send the IP address. The connection is dropped immediately after the IP address has been sent. This connection is subject to the usual charges.
- ③ Gateway 2 connects to the ISP and receives a dynamic IP address.
 - ④ Gateway 2 now sets up the VPN tunnel to Gateway 1.



ELSA LANCOM Dynamic VPN works only between ELSA LANCOM that each feature at least one ISDN port that can be used for the ISDN connection.

1.5

An overview of **ELSA LANCOM VPN**

This section lists all of the functions and properties of *ELSA LANCOM VPN*. This overview will provide a great deal of information for VPN experts. It is very compact, but contains a great deal of complex, specialized terminology. Knowledge of the technical basics of VPN are required to understand this section. Don't worry: it's no problem if you skip this section. The information contained here is not required to set up and use *ELSA LANCOM VPN*.

- VPN in accordance with IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- *ELSA LANCOM Dynamic VPN*: Public IP addresses can be static or dynamic (ISDN connection required)
- Supported connection technologies:

Device	Connection technology	Comments
<i>ELSA LANCOM Business 4000</i>	ISDN	
<i>ELSA LANCOM Business 4100</i>	ISDN (4 x)	
<i>ELSA LANCOM Business 6001</i>	X.21, ISDN	backup via ISDN
<i>ELSA LANCOM Business 6011</i>	G.703, X.21, ISDN	backup via ISDN
<i>ELSA LANCOM Business 6021</i>	G.703 (2 x), X.21, ISDN	backup via ISDN
<i>ELSA LANCOM DSL/I-1610 Office</i>	10Base-T (DSL, cable modem etc.)	<i>ELSA LANCOM Dynamic VPN</i> not possible
<i>ELSA LANCOM DSL/I-1611 Office</i>	10Base-T (DSL, cable modem etc.), ISDN	backup via ISDN

- IPsec protocols AH and ESP in transport and tunnel mode
- Hash algorithms:
 - HMAC-MD5-96, Hash length 128 bit
 - HMAC-SHA-1-96, Hash length 160 bit
- Symmetrical encryption methods
 - DES-CBC, key length 56 bit
 - Triple-DES-CBC, key length 112 bit
 - CAST-CBC, key length 128 bit
 - Blowfish-CBC, key length 128 bit
- Mutual authentication through preshared keys
- Key exchange via Oakley, encryption in accordance with Diffie-Hellman, support of well-known groups 1 to 5 (key lengths 768 bit, 1024 bit, 1536 bit, elliptical curves with $GF(2^{155})$ and $GF(2^{185})$)
- Key management in accordance with ISAKMP

1.6

What now?

The following chapter will describe the installation of the *ELSA LANCOM VPN Option* on a *ELSA LANCOM*.

As soon as the *ELSA LANCOM VPN Option* is installed on the desired *ELSA LANCOM*, go to 'Setting up the VPN connection' on page 27 for the steps needed to establish VPN connections.

2 Installation of the VPN option

This chapter will explain how to install *ELSA LANCOM VPN Option* in your *ELSA LANCOM*. The installation takes place in six steps:

- ① Checking the installation requirements
- ② Online registration
- ③ Updating the *ELSA LANtools* (*ELSA LANconfig*, *ELSA LANmonitor*)
- ④ Uploading the current firmware
- ⑤ Activating the VPN option
- ⑥ Checking the activation

2.1 Installation requirements

Please take a few minutes to check whether all of the requirements for a successful installation have been fulfilled.

2.1.1 Supported **ELSA LANCOM**

The *ELSA LANCOM VPN Option* is supported by the following *ELSA LANCOM*:

- *ELSA LANCOM Business 4000*
- *ELSA LANCOM Business 4100*
- *ELSA LANCOM Business 6001*
- *ELSA LANCOM Business 6011*
- *ELSA LANCOM Business 6021*
- *ELSA LANCOM DSL/1610 Office (without ELSA LANCOM Dynamic VPN)*
- *ELSA LANCOM DSL/I-1611 Office*

2.1.2 Package contents

Please ensure that the package contains the following components:

- *ELSA LANCOM VPN CD* with *ELSA LANtools*, current firmware and electronic documentation
- Yellow sticker with printed serial number
- User manual

2.1.3

Access to the device and *ELSA LANconfig*

To install the *ELSA LANCOM VPN Option*, you need a computer with a Windows operating system (Windows 95, Windows 98, Windows NT 4.0, Windows 2000 or Windows Millennium Edition). This computer must have access to the *ELSA LANCOM* to be configured. The device's integrated serial configuration port (outband), the LAN (inband) or remote configuration are the available access options.

The *ELSA LANconfig* version 1.65 or higher configuration program must be installed on the computer. If you already have *ELSA LANconfig* installed on this computer, please check the version. For further information on checking the software version, please see the next section.

Launching and using *ELSA LANconfig* is described in detail in the documentation of your *ELSA LANCOM*.

2.1.4

Checking the *ELSA LANconfig* version

Please ensure that you are using *ELSA LANconfig* version 1.65 or higher. The version number can be found under the menu **Help ► About ELSA LANconfig**.

Version 1.65 of the *ELSA LANtools* can be found on the *ELSA LANCOM VPN* CD and can be installed on your computer with the **SETUP** program if required.

The latest versions of ELSA LANconfig and ELSA LANmonitor can be found on the ELSA web site at www.elsa.com in the file section ('Download').



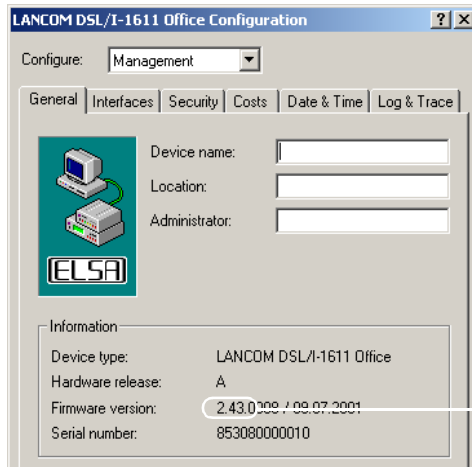
2.1.5

Checking the firmware version

The firmware of your *ELSA LANCOM* must support *ELSA LANCOM VPN*. Depending on your device, at least the following firmware versions must be installed:

Device	Firmware
<i>ELSA LANCOM Business 4000/4100</i>	Version 2.21
<i>ELSA LANCOM Business 6001/6011/6021</i>	Version 2.21
<i>ELSA LANCOM DSL/-1610 Office</i>	Version 2.41
<i>ELSA LANCOM DSL/-1611 Office</i>	Version 2.41

You can easily determine the firmware version of your *ELSA LANCOM*. In the *ELSA LANconfig* selection list, double-click the required *ELSA LANCOM*. A configuration window will open containing the firmware version:



The first digits show the current firmware version

2.1.6

Updating the firmware

This section is only relevant if you have checked the firmware version of your device and have determined that you need a later version.

The current firmware version for all supported devices can be found on the *ELSA LANCOM VPN Option* CD in the 'Firmware' folder. This folder contains subfolders for the various devices of the *ELSA LANCOM* series, for example 'Firmware\4x00\' for the devices of the 4000/4100 series. There you can find a file with the ending '.221', for example, that contains the required firmware.

The latest firmware updates can be found on the ELSA web site at www.elsa.com in the file section ('Download'). Find your device in the list of devices and download the file with the current firmware version to your computer.

You can find information on installing the new firmware on the *ELSA LANCOM* in your device manual.



2.2 Online registration

With the correct firmware version, your *ELSA LANCOM* already contains the complete VPN software. It only needs to be activated.

An activation code is required to enable the VPN option in your *ELSA LANCOM*.



Please note: *The activation code is not included in the package, but will be sent to you during the online registration.*

A license certificate (yellow sticker) is included with your *ELSA LANCOM VPN Option*. A license number is printed on this sticker. With this license number, you can register with ELSA to receive your activation code.



A successful online registration cancels the used license number of your ELSA LANCOM VPN Option. The activation code that you will receive during registration can only be used on the ELSA LANCOM with the specified serial number! Please make sure that you want to install the VPN option on the specified device. It will not be possible to switch to a different device at a later time!

Please have the following information on hand for the online registration:

- Exact designation of the software option
- The license number (from the yellow license sticker)
- Serial number of the *ELSA LANCOM* to be activated (on the underside of the device)
- Your customer information (company, name, address, e-mail).



The registration can also be done anonymously, without supplying personal information. The additional information assists us in providing support and service, however. We regard all supplied information to be strictly confidential, of course.

Launch your web browser and go to the following web page:

<http://www.elsa.com/register/routeroption>

Enter the information listed above in the form and follow the additional instructions on the page. After you have entered your information, a page will be displayed containing the activation code for the VPN option of your *ELSA LANCOM*, as well as your customer information. Please print this page using the print function of your web browser. If you have supplied your e-mail

address, the information and your activation code will also be sent to you via e-mail. The online registration is now complete.

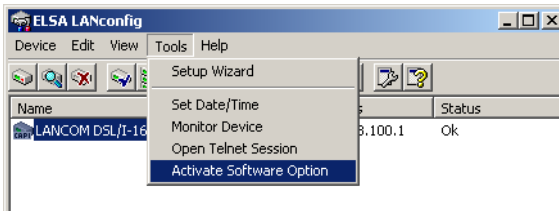
Please store your activation code in a safe place! You may need it again to restore the VPN option, after a repair for example.



2.3

Activating the VPN option

The VPN option is very easy to activate. In *ELSA LANconfig*, select the required *ELSA LANCOM* (single click on the entry) and select **Tools** ► **Activate Software Option** menu item:



The 'Activate Software Option' or 'Activate Additional Feature' dialog box will appear:



Enter the activation code you have received during the online registration described above. Next, the *ELSA LANCOM* will reboot.

2.4 Checking the activation

You can verify the successful activation of the *ELSA LANCOM VPN Option* by selecting the device in *ELSA LANconfig* and selecting the **Device ► Properties** menu item. The 'Information' tab of the properties window will display a list of the active software options.

3 Setting up the VPN connection

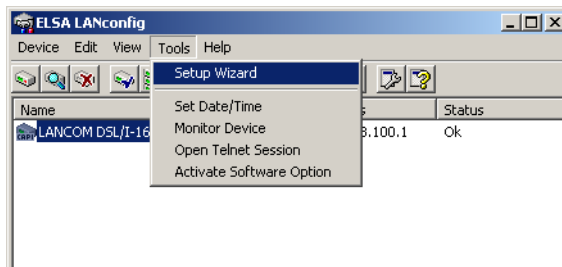
Once you have installed *ELSA LANCOM VPN Option* on the desired *ELSA LANCOM*, this chapter will provide you with all of the information needed to set up a VPN connection.

This chapter is organized in six sections:

- Using the *ELSA LANconfig* Wizard for VPN
- What information is required for the VPN connection?
- Examples of VPN configurations
- Setting up the basic connection
- Before entering the VPN connection data
- Entering the data and testing the VPN connection

3.1 The *ELSA LANconfig* Wizard for VPN

VPN connections can be established with the *ELSA LANconfig* Setup Wizard. To start the wizard, highlight the desired *ELSA LANCOM* and select the **Tools ► Setup Wizard** menu item:



A window then appears with the wizard available for that device.

The use of the wizard is intuitive. All of the parameters needed for the desired connection are queried step by step. **Next** and **Back** can be used to navigate between the windows at any time.

The wizard for VPN connections: connecting two local networks

A separate wizard is not available for VPN. Instead, the existing LAN-LAN Coupling Wizard ('Connect two local area networks') is used. With the

activation of *ELSA LANCOM VPN*, the VPN queries are added to the LAN-LAN Wizard.

Converting existing connections to VPN connections

To convert existing network couplings to VPN connections, we recommend running the LAN-LAN Wizard completely a second time.

When you are asked for your own device name or that of the remote station, use the same names that the old network coupling uses. Be sure to write them in exactly the same way.

The previous network connection will then be replaced by a VPN-based network connection.

3.2 What will the wizard ask?

It is very useful to collect all of the required information about the involved devices before starting the wizard. Here is an overview of the information needed by the wizard.

3.2.1 Overview of configuration entries

This overview contains all of the questions that the wizard will ask you during the installation. Some questions are not required for certain configurations. We will explain all of the questions nevertheless, but will point out the cases in which they are unnecessary.

A VPN connection always exists between the device to be configured and a known remote station. The configuration is performed on both sides. Care must be taken to ensure that the configuration information provided matches.

The overview also shows the dependencies of the information between the two stations. Noting these dependencies can prevent many incorrect entries.

Entry	Gateway 1		Gateway 2
VPN via direct connection or Internet?	<i>direct/Internet</i>	↔	<i>direct/Internet</i>
Type of the local IP address	<i>static/dynamic</i>	↔	<i>static/dynamic</i>
Type of the remote IP address	<i>static/dynamic</i>	↔	<i>static/dynamic</i>
Name of the local device	<i>name1</i>	↔	<i>name2</i>
Name of the remote station	<i>name2</i>	↔	<i>name1</i>

Entry	Gateway 1	Gateway 2
Interface for direct connection	<i>interface1</i>	<i>interface2</i>
Remote ISDN calling number	<i>phone number1</i>	<i>phone number2</i>
Remote ISDN caller ID	<i>ISDN ID1</i>	<i>ISDN ID2</i>
Password for ISDN connection	<i>password1</i>	↔ <i>password1</i>
Shared Secret for encryption	<i>secret</i>	↔ <i>secret</i>
Data compression	<i>on/off</i>	↔ <i>on/off</i>
Channel bundling	<i>on/off</i>	↔ <i>on/off</i>
IP address of remote station	<i>IP address1</i>	<i>IP address2</i>
IP network address of the remote network	<i>IP address3</i>	<i>IP address4</i>
Netmask of the remote network	<i>IP netmask to IP address3</i>	<i>IP netmask to IP address4</i>
Access to stations in local network permitted?	<i>yes = Intranet no = Extranet</i>	<i>yes = Intranet no = Extranet</i>
NetBIOS routing for access to remote network?	<i>yes/no</i>	<i>yes/no</i>
Name of remote workgroup (NetBIOS only)	<i>workgroup1</i>	<i>workgroup2</i>



The 'Gateway 1' and 'Gateway 2' columns contain selection options and variables as placeholders for actual configuration information. Unlike actual entries, these placeholders are italicized.

The column between the variables marks required dependencies that must be taken into consideration when making the entries at both gateways. For example, the entries stating whether the VPN connection should be established using a direct connection or via the Internet must be the same for both gateways. Places where the entries must match are marked by arrows (↔).

This table only provides an initial overview of the possible configuration entries. The following section describes the individual configuration entries in detail.

That is followed by a section with descriptions of sample configurations for the most important configuration types. A table with actual input values is provided for each version. Simply select the most suitable version for yourself from this section. The associated table will show you the information required for your configuration at a glance.

3.2.2

Meaning of the configuration entries



All queries are covered in detail in this section. They have been grouped according to topic to improve the overview.

Direct connection or connection over the Internet?

	Gateway1		Gateway2
VPN via direct connection or over the Internet?	<i>direct/Internet</i>	↔	<i>direct/Internet</i>

VPN tunnels can be established via direct connections (i.e. dedicated switched or fixed connections) between the networks and over the Internet. Depending on the *ELSA LANCOM*, the following connection technologies are supported: ADSL, SDSL, cable modem, ISDN, X.21, G.703.

General information on the local device and the remote station

Type of the local IP address	<i>static/dynamic</i>		<i>static/dynamic</i>
Type of the remote IP address	<i>static/dynamic</i>		<i>static/dynamic</i>
Name of the local device	<i>name1</i>		<i>name2</i>
Name of the remote station	<i>name2</i>		<i>name1</i>

The type of IP address must be stated for both sides for VPN connections via the Internet (not for direct connections). There are two **types of IP addresses**: static and dynamic. For an explanation of the two IP address types, please see the section 'Send your data through the tunnel—for security's sake' on page 11.

The local IP address type and that of the remote station must be entered. Both entries must match.

Providing a local **device name** renames your *ELSA LANCOM*. The device will appear with the selected name in the device list of *ELSA LANconfig* and *ELSA LANmonitor*. If you would like to retain the previous name of your device, enter it here.

Connection information

Interface for direct connection	<i>interface1</i>		<i>interface2</i>
Remote ISDN calling number	<i>phone number1</i>		<i>phone number2</i>
Remote ISDN caller ID	<i>ISDN ID1</i>		<i>ISDN ID2</i>
Password for ISDN connection	<i>password1</i>	↔	<i>password1</i>

When providing information on the connection, three cases must be distinguished depending on the VPN connection type:

- The VPN connection based on a direct connection between the stations, i.e. not via the Internet.
- An Internet connection, with one side using a dynamic IP address. In this case, *ELSA LANCOM Dynamic VPN* will need additional information for the ISDN connection used to transfer the IP address.
- VPN tunnels via completely static Internet connections do not need these four additional items of information to set up a connection. In the case of completely static Internet connections, the remote station is addressed via its public IP address (see 'The IP address of the remote station' on page 33).

The specified **interface** is used for ISDN connections to the remote station. Stating the interface is necessary not only for direct connections, but also for VPN connections via the Internet when the remote station only has a dynamic IP address.

Enter the calling number of the remote station in the **ISDN calling number** field. The complete calling number including all necessary area and country codes is required. If your device is connected to the ISDN via a PBX system, a prefix generally will be needed for an external call (usually '0').

If the VPN tunnel is to be set up via a leased ISDN line, enter an 'F' for 'fixed connection' instead of the calling number.

Setting up a fixed ISDN connection generally requires additional settings in the advanced configuration. Please refer to the device manual for more information.

The stated **ISDN caller ID** is used to identify and authenticate callers. An identification is performed for all ISDN calls: for direct ISDN connections as well as for all Internet connections in which your local device only has a dynamic IP address.



When an *ELSA LANCOM* receives a call, it compares the ISDN caller ID entered for the remote station with the actual caller ID transferred via the D-channel. An ISDN caller ID generally consists of an area code and an MSN.

The **password for the ISDN connection** is an alternative to the use of the ISDN caller ID. It is always used to authenticate callers that do not send an ISDN caller ID. The exact same password must be entered on both sides. It is used for calls in both directions.

The Shared Secret

Shared Secret for encryption	Shared Secret	↔	Shared Secret
------------------------------	---------------	---	---------------

The Shared Secret is the central password for security within the VPN tunnel. Strictly speaking, it is not used for encryption, but simply for mutual authentication. The security of the VPN connection is affected decisively by the Shared Secret.

The Shared Secret must not be confused with a connection password. The Shared Secret is used for mutual authentication when setting up the logical VPN tunnel. The connection password is already used during the establishment of the physical connection to the remote station. For more information on the connection password, please refer to 'Connection information' on page 31.

A number of basic rules must be observed for the handling of passwords. These also apply to the Shared Secret:

- **Keep your password as secret as possible.**

Never write a password down. Popular, but completely unsuitable storage options include: notebooks, wallets, and text files in your computer. It sounds trivial, but it can't be repeated often enough: Do not pass on your password. The most secure systems surrender to talkativeness.

- **Only send passwords in a secure manner.**

A selected password must be reported to the other side. To do this, select the most secure method possible. Avoid: unprotected e-mail, letter, fax. It is better to convey a password personally while alone with the other person. The maximum security is achieved when you personally enter the password at both ends.

- **Select a secure password.**

Use randomly chosen letter and number sequences. Passwords from



common language usage are not secure. Special characters such as '&"?#*+_.,!@' also make it more difficult for attackers to guess your password and increase the security of the password.

- **Never use a password twice.**

If you use the same password for several purposes, you reduce its security effect. If one station is insecure, this automatically jeopardizes the security of all other connections that use the same password.

- **Change the password regularly.**

Passwords should be changed as frequently as possible. This requires effort, however considerably increases the security of the password.

- **Change the password immediately if you suspect someone else knows it.**

If an employee with access to a password leaves the company, it is high time to change this password. A password should also always be changed when there is the slightest suspicion of a leak.

If you comply with these simple rules, you will achieve the highest possible degree of security with the Shared Secret.

Data compression and channel bundling

Data compression	on/off	↔	on/off
Channel bundling	on/off	↔	on/off

When setting up a direct VPN connection, the LAN-LAN Wizard offers two advanced connection options: data compression, and the bundling of two connection channels via MLPPP (**M**ulti**L**ink **P**PP). These options can increase the transfer speed of the connection.

Data compression and channel bundling can also be used for VPN connections via the Internet. The necessary settings are not made in the LAN-LAN Wizard, but in the Internet Wizard when setting up Internet access.

The IP address of the remote station

IP address of remote station	IP address1	IP address2
------------------------------	-------------	-------------

The **IP address of the remote station** is required to set up the VPN connection in the following situations:



- For direct connections via fixed or switched lines, enter the private IP address of the remote *ELSA LANCOM*.
- For a VPN connection via the Internet to a remote station with a static address, enter its public IP address.
- If the remote station only has a dynamic IP address, its public IP address will not be known until the connection is made. The wizard does not ask for the IP address for this reason.

Routing settings

IP network address of the remote network	<i>IP address3</i>		<i>IP address4</i>
Netmask of the remote network	<i>IP netmask to IP address3</i>		<i>IP netmask to IP address4</i>
Access to stations in local network permitted?	<i>yes = Intranet no = Extranet</i>		<i>yes = Intranet no = Extranet</i>

The routing settings are not specific to VPN connections, but are required for all LAN-LAN couplings.

The **IP address of the remote network** is always entered together with the associated **netmask**.

You can thus limit **access to your own network**. In the intranet mode, the remote network has complete access to your local network at the IP level. In the extranet mode, the stations of the remote network do not have access to your local network.

Routing for NetBIOS

NetBIOS routing for access to remote network?	<i>yes/no</i>		<i>yes/no</i>
Name of remote workgroup (NetBIOS only)	<i>workgroup1</i>		<i>workgroup2</i>

The information for NetBIOS routing is also not VPN-specific, but is queried at the IP level for all LAN-LAN couplings.

The NetBIOS protocol is used by some network systems for access to shared resources (mostly servers and printers). A common example for the use of NetBIOS: Windows networks.

3.3 Examples of VPN configurations

This section covers the most important types of VPN connections. The required configuration information for each VPN connection type can be found in the familiar table form.



The tables only contain the required information. For example, in the case of static Internet connections, parameters for the ISDN connection are not stated. NetBIOS information is also not provided. In all examples, the tunnels are set up between two ELSA LANCOMs. Direct connections and Internet access are realized via ISDN (using the first S_0 port). Devices of the ELSA LANCOM Business 6000 series can also use a 2-Mbit port. All depicted LANs use the netmask 255.255.0.0.

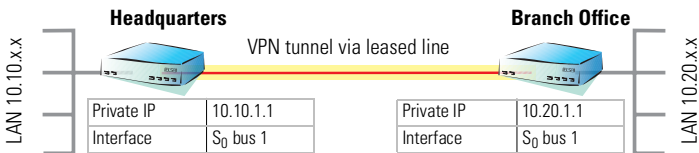
3.3.1 VPN via direct connection

We will group the first two connection types under the term “direct connection”:

- Leased line (fixed connection) via ISDN or G.703
- ISDN dial-up connection

These connections are established directly between the two connected devices.

VPN connection via leased line



The *ELSA LANCOM* **Headquarters** and **Branch Office** devices are connected via a leased line.

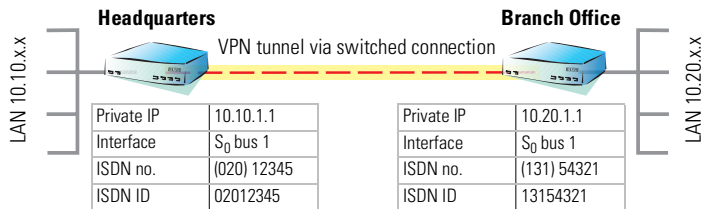
	Headquarters	Branch Office
VPN via direct connection or Internet?	direct	direct
Name of the local device	Headquarters	Branch Office
Name of the remote station	Branch Office	Headquarters
Interface	S_0 bus 1	S_0 bus 1

	Headquarters	Branch Office
Remote ISDN calling number	F	F
Shared Secret for encryption	<i>secret</i>	<i>secret</i>
IP address of remote station	10.20.1.1	10.10.1.1
IP network address of the remote network	10.20.0.0	10.10.0.0
Netmask of the remote network	255.255.0.0	255.255.0.0



Setting up a fixed ISDN connection generally requires additional measures in the advanced configuration of ELSA LANconfig. Please refer to the device manual for more information.

VPN via switched connection



In the example, the **ELSA LANCOM Headquarters** and **Branch Office** are connected via a direct switched ISDN connection.

	Headquarters	Branch Office
VPN via direct connection or Internet?	direct	direct
Name of the local device	Headquarters	Branch Office
Name of the remote station	Branch Office	Headquarters
Interface	S ₀ bus 1	S ₀ bus 1
Remote ISDN calling number	13154321	02012345
Remote ISDN caller ID	02012345	13154321
Password for ISDN connection	<i>confidential</i>	<i>confidential</i>
Shared Secret for encryption	<i>secret</i>	<i>secret</i>
IP address of remote station	10.20.1.1	10.10.1.1
IP network address of the remote network	10.20.0.0	10.10.0.0
Netmask of the remote network	255.255.0.0	255.255.0.0

3.3.2

VPN via the Internet

For VPN connections via the Internet, the IP address type on both sides plays an important role for the configuration. We distinguish between three different cases:

- static/static
- static/dynamic
- dynamic/dynamic



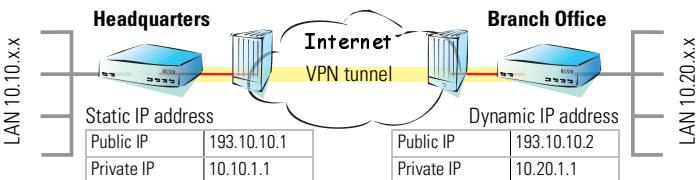
When setting up a VPN connection via the Internet please be sure that the LAN-LAN Wizard does not set up a new Internet connection. An Internet access must be already set up before running the LAN-LAN Wizard. The correct functioning of this Internet access must also be tested before setting up the VPN connection.



If multiple Internet connections are available, use the one associated with the default route (255.255.255.255) in the routing table.

In the following examples, the connection is made to the Internet service provider via a leased line for devices with a static IP address and via a switched ISDN connection for devices with a dynamic IP address. The connection type to the ISP is not relevant for the configuration at this point and can easily be altered as required.

static/static

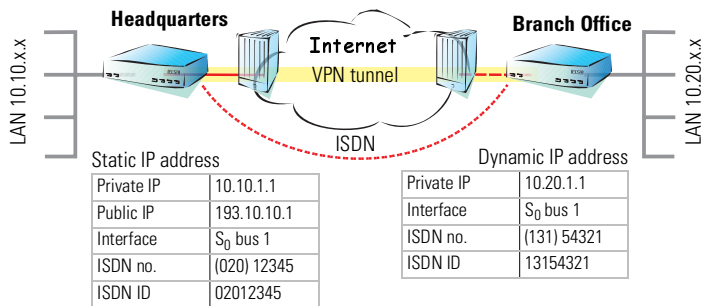


A VPN tunnel via the Internet serves as the connection between the *ELSA LANCOM Headquarters* and **Branch Office**. Both gateways have static IP addresses.

Entry	Headquarters	Branch Office
VPN via direct connection or Internet?	Internet	Internet
Type of the local IP address	static	static
Type of the remote IP address	static	static

Entry	Headquarters	Branch Office
Name of the local device	Headquarters	Branch Office
Name of the remote station	Branch Office	Headquarters
Shared Secret for encryption	<i>secret</i>	<i>secret</i>
IP address of remote station	193.10.10.2	193.10.10.1
IP network address of the remote network	10.20.0.0	10.10.0.0
Netmask of the remote network	255.255.0.0	255.255.0.0

static/dynamic



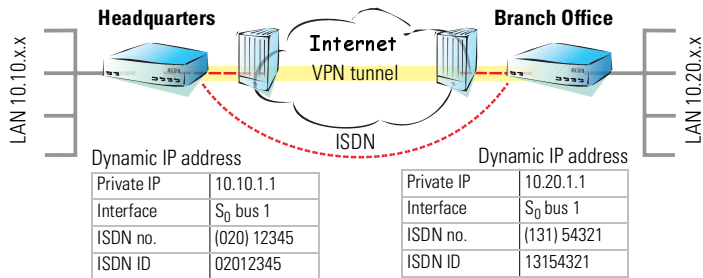
A VPN tunnel via the Internet serves as the connection between the *ELSA LANCOM* **Headquarters** and **Branch Office**. **Headquarters** has a static IP address, **Branch Office** a dynamic address.

The details of the ISDN connection are used for the transmission of the IP address, not for the actual connection to the Internet. The Internet connection is configured with the Internet Access Wizard.

Entry	Headquarters	Branch Office
VPN via direct connection or Internet?	Internet	Internet
Type of the local IP address	static	dynamic
Type of the remote IP address	dynamic	static
Name of the local device	Headquarters	Branch Office
Name of the remote station	Branch Office	Headquarters
Interface	S ₀ bus 1	S ₀ bus 1
Remote ISDN calling number	13154321	02012345
Remote ISDN caller ID	02012345	13154321

Entry	Headquarters	Branch Office
Password for ISDN connection	<i>confidential</i>	↔ <i>confidential</i>
Shared Secret for encryption	<i>secret</i>	↔ <i>secret</i>
IP address of remote station		193.10.10.1
IP network address of the remote network	10.20.0.0	10.10.0.0
Netmask of the remote network	255.255.0.0	255.255.0.0

dynamic/dynamic



A VPN tunnel via the Internet serves as the connection between the *ELSA LANCOM Headquarters* and **Branch Office**. Both sides have dynamic IP addresses.

The details of the ISDN connection are used for the transmission of the IP address, not for the actual connection to the Internet. The Internet connection is configured with the Internet Access Wizard.

Entry	Headquarters	Branch Office
VPN via direct connection or Internet?	Internet	↔ Internet
Type of the local IP address	dynamic	↔ dynamic
Type of the remote IP address	dynamic	↔ dynamic
Name of the local device	Headquarters	↔ Branch Office
Name of the remote station	Branch Office	↔ Headquarters
Interface	S ₀ bus 1	S ₀ bus 1
Remote ISDN calling number	13154321	02012345
Remote ISDN caller ID	02012345	13154321
Password for ISDN connection	<i>confidential</i>	↔ <i>confidential</i>

Entry	Headquarters		Branch Office
Shared Secret for encryption	<i>secret</i>	↔	<i>secret</i>
IP network address of the remote network	10.20.0.0		10.10.0.0
Netmask of the remote network	255.255.0.0		255.255.0.0

3.4 Setting up the basic connection

The LAN-LAN Wizard will not automatically set up and configure the basic connection (leased, switched or Internet connection) in every case. In some cases, additional configuration steps are required.

3.4.1 Direct connections

Direct switched connections are completely set up by the LAN-LAN Wizard. Modifications to the advanced configuration are generally not necessary.

Additional configuration steps are also not required for direct fixed connections via 2-Mbit lines (G.703, X.21). The situation is different for fixed ISDN connections: they generally require extensive adaptation of the advanced configuration. The documentation of your device contains all of the required information.

3.4.2 Connections via the Internet

The LAN-LAN Wizard does not set up Internet access. It requires a working Internet connection, which it then uses. This connection can be set up using the Internet Access Wizard. The Internet access should be fully configured before starting on the VPN connection with the LAN-LAN Wizard.

Switched connections to the Internet can be set up fully using the Internet Access Wizard. Fixed connections via 2-Mbit interfaces (G.703, X.21) also do not require any additional steps.

When using a leased ISDN line, enter an 'F' for 'fixed connection' instead of the calling number in the wizard. Generally, additional configuration steps are required. Please refer to the device manual for more information.

The VPN connection always uses the 'DEFAULT' Internet access. The IP address 255.255.255.255 must therefore be assigned to the desired connection in the routing table.

Multiple Internet connections can be set up in the *ELSA LANCOM* that can be used alternatively depending on the time of day.

3.5 Before entering the VPN connection data

Please ensure that the following requirements are met before running the LAN-LAN Wizard to set up a VPN network coupling:

- The *ELSA LANCOM VPN Option* has been activated on both *ELSA LANCOMs*.
- You have all required configuration information.
- If the VPN connection is to be set up via the Internet, both *ELSA LANCOMs* must have fully configured, working Internet connections.

3.6 Entering the data and testing the VPN connection

Launch the LAN-LAN Wizard and enter the required configuration information.

After running the wizard on both sides, you can test the VPN connection. Send a PING from your network to any computer in the remote network.

4 The technology behind VPN

This chapter explains the technical fundamentals of VPN in general and *ELSA LANCOM VPN* in particular. It will provide an overview of the concepts used and the standards on which the technology is based.

This knowledge is not absolutely essential for the use of VPN with *ELSA LANCOM*, but it can be helpful. *ELSA LANCOM VPN* is designed to let you take advantage of VPN technology without specialized knowledge. VPN connections in particular can be set up without detailed background knowledge.

4.1 How does VPN work?

In practice, a VPN must fulfill a number of requirements:

- Unauthorized third parties must not be able to read the data (encryption)
- It should not be possible to manipulate the data (data integrity)
- Unambiguous identification of the sender of data (authentication)
- Simple key management
- Compatibility to VPN devices from a variety of manufacturers

ELSA LANCOM VPN achieves these five major goals by applying the widely used IPSec standard.

4.1.1 IPSec—the foundation of *ELSA LANCOM VPN*

The original IP protocol does not contain any provisions for security. Security problems are compounded by the fact that IP packets do not go directly to a specific recipient, but are sent scattershot to all computers on a given network segment. Anyone can help themselves and read the packets. This leaves the door open to the misuse of data.

IP has been developed further for this reason. A secure version is now available: IPSec. *ELSA LANCOM VPN* is based on IPSec.

IPSec stands for “**IP Security Protocol**”, which was originally the name of a project group within the IETF, the **I**nternet **E**ngineering **T**ask **F**orce. Over the years, this group has developed a framework for a secure IP protocol that is generally referred to as IPSec today.

It is important to note that IPSec itself is not a protocol, but merely the standard for a protocol framework. IPSec actually consists of a variety of protocols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

Security in an IP environment

IPSec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPSec thus replaces the IP protocol. Under IPSec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPSec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPSec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function-dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPSec.

IPSec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPSec will remain the most important standard for virtual private networks in the future.

4.1.2

Alternatives to IPSec

IPSec is an open standard. It is not dependent on individual manufacturers and is being developed by the IETF with input from the interested public. The IETF is a nonprofit organization that is open to everyone. The broad acceptance of IPSec is the result of this open structure which unites a variety of technical approaches.

Nevertheless, there are other approaches for the realization of VPNs. We will only mention the two most important of these here. They are not realized at the network level like IPSec, but at the connection and application levels.

Security at the connection level—PPTP, L2F, L2TP

Tunnels can already be set up at the connection level (level 2 of the OSI model). Microsoft and Ascend developed **P**oint-to-**P**oint **T**unneling **P**rotocol

(PPTP) early on. Cisco introduced a similar protocol with **Layer 2 Forwarding (L2F)**. Both manufacturers agreed on a joint approach which then became the **Layer 2 Tunnel Protocol (L2TP)** in the IETF.

The objective of the protocols is to ensure security when dialing into networks and replace the PPP and SLIP standards. Their main advantage over IPSec is that any network protocol can be used with such a network connection, especially NetBEUI and IPX.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections. L2TP can also be combined with IPSec to provide enhanced security for dial-up connections.

Security at higher levels—SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Common examples for protocols of this type are SSL (**Secure Socket Layer**), mainly for Web browser connections, S/MIME (**Secure Multipurpose Internet Mail Extensions**) for e-mail and PGP (**Pretty Good Privacy**) for e-mail and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols is the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPSec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred. They are usually much more complex, however.

All of these layer-4 protocols only support end-to-end connections; they are therefore not suitable for coupling entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

Combinations are possible

All of the alternatives listed above are compatible to IPSec and can therefore be used parallel to it. This permits a further increase of the security level. It would be possible, for example, to dial into the Internet using an L2TP connection, set up an IPSec tunnel to a Web server and exchange HTTP data between the Web server and the browser in secure SSL mode.

Each additional encryption would reduce the data throughput, however. Users can decide on a case-by-case basis whether the security offered by IPSec alone is sufficient. Higher security will only be required rarely, since the degree of required security can also be set within IPSec.

4.2 The standards behind IPSec

IPSec is based on a variety of protocols for the individual functions. These protocols are based on, and complement one another. The modularity achieved with this concept is an important advantage of IPSec over other standards. IPSec is not restricted to specific protocols but can be supplemented at any time by future developments. The protocols integrated to date also offer such a high degree of flexibility that IPSec can be perfectly adapted to virtually any requirements.

4.2.1 IPSec modules and their tasks

IPSec has to perform a number of tasks. One or more protocols have been defined for each of these tasks.

- Authentication of packets
- Encryption of packets
- Transfer and management of keys

4.2.2 Security associations—numbered tunnels

A logical connection (tunnel) between two IPSec devices is known as an SA (**S**ecurity **A**ssociation). SAs are managed independently by the IPSec device. An SA consists of three values:

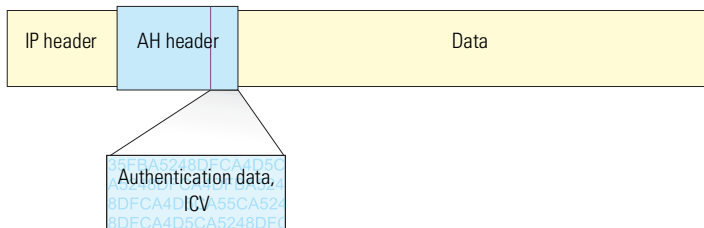
- **Security Parameter Index (SPI)**
ID to distinguish multiple logical connections to the same target device with the same protocols

- Designates the security protocol used for the connection: AH or ESP (further information will be provided on these protocols in the following sections).

The SAs are managed in an internal database of the IPsec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

Authentication—the AH protocol

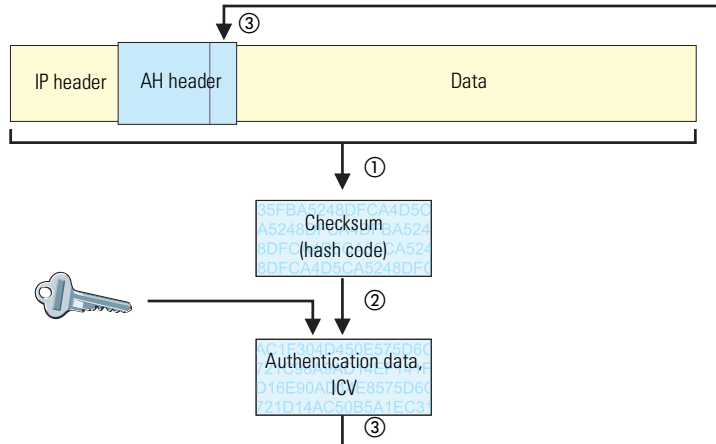
AH adds its own header to IP packets immediately after the original IP header. The most important part of this AH header is a field containing authentication data, often referred to as the **Integrity Check Value (ICV)**.



In the sender, the authentication data is generated in 3 steps.

- ① A checksum is calculated for the complete package using a hash algorithm.

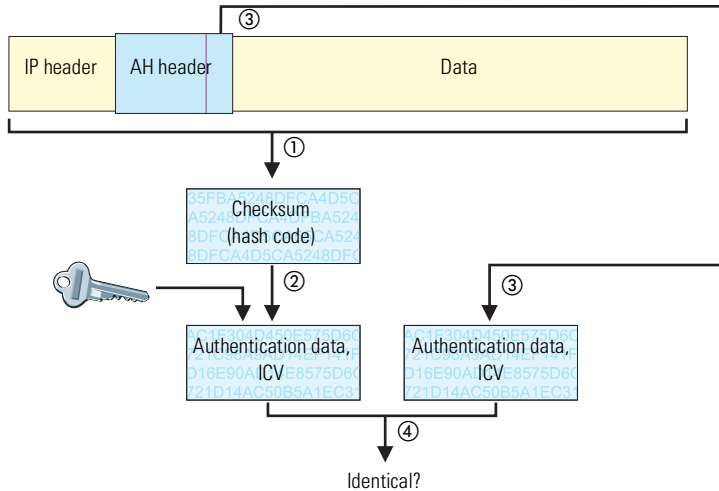
- ② This checksum is once again sent through a hash algorithm together with a key known to both the sender and the recipient.
- ③ This results in the required authentication data which is inserted in the AH header.



Checking of integrity and authenticity by the recipient

The AH protocol works in a very similar manner at the recipient's end. The recipient also uses his key to calculate the authentication data for the

received packet. The comparison with the sent ICV of the packet determines the integrity and authenticity of the packet.



Determining the checksum for the integrity check

AH adds a checksum to each packet before it is sent to guarantee the integrity of the transferred packets. At the recipients end, AH checks whether the checksum and the contents of the package match. If this is not the case, the packet was either incorrectly transferred or deliberately manipulated. Such packets are discarded immediately and are not forwarded to higher protocol levels.

A variety of so-called hash algorithms are available to determine the checksum. Hash algorithms are distinguished by the fact that their results (the hash code) are a unique fingerprint of the original data. Conversely, the original data cannot be determined on the basis of the hash code.

ELSA LANCOM VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods work without keys, i.e. on the basis of fixed algorithms. Keys do not play a role until a later step of AH: the final generation of the authentication data. The integrity checksum is only a necessary intermediate result on the way there.

Generation of the authentication data

In the second step, AH generates a new hash code using the checksum and a key—the final authentication data. A variety of standards are available under IPSec for this process as well. *ELSA LANCOM VPN* supports HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly known as HMAC-MD5-96 and HMAC-SHA-1-96.

This clarifies why AH leaves the packet itself unencrypted. Only the checksum of the packet and the local key are added to the packet together with the ICV, the authentication data, in encrypted form as a verification criterion.

Replay protection—protection against replayed packets

In addition to the ICV, AH assigns a unique sequence number to each packet. The recipient can thus recognize which packets were intercepted by a third party and resent. Attacks of this type are known as “packet replay”.

The sender adds such a sequence number to each packet by default before sending it on its way. If the recipient decides that replay protection is not required, the sender stops numbering the packets.

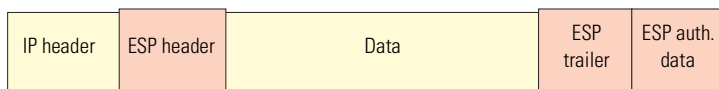
4.2.4

Encryption of the packets—the ESP protocol

The ESP protocol (**E**ncapsulating **S**ecurity **P**ayload) encrypts the packets as protection against unauthorized access. This was once the only function of ESP, but in the course of the further development of the protocol it was expanded with options for the protection of integrity and verification of authenticity. In addition, ESP also features effective protection against replayed packets. ESP thus offers all of the functions of AH—in some cases, however, the use of AH parallel to ESP is advisable.

How ESP works

The structure of ESP is more complex than that of AH. ESP also inserts a header behind the IP header as well its own trailer and a block of ESP authentication data.



Transport and tunnel mode

Like AH, ESP can be used in two modes: transport and tunnel mode.

In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted.

The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for the remote configuration of a router, for example. It cannot be used for the coupling of networks via the Internet—this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

Encryption algorithms

As a higher-level protocol, IPSec does not require specific encryption algorithms. The manufacturers of IPSec products are thus free in their choice of the processes used. *ELSA LANCOM VPN* currently supports the following common standards:

- **DES—Data Encryption Standard**

DES was developed by IBM for the NSA (National Security Agency) in the early 1970s and was the worldwide security standard for years. The key length of this symmetrical process is 56 bits. Today, it is considered to be insecure due to its short key length and should therefore not be used if possible.

- **Triple-DES (also 3DES)**

A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. The form of Triple-DES algorithm used by *ELSA LANCOM VPN* uses two different keys for the three DES runs. The key for the first run is reused for the third DES run. The result is an effective key length of 112 bits.

Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be highly secure. Triple-DES is slower than other processes, however.

- **CAST** (named after its authors, **C**arlisle **A**dams and **S**tafford **T**avares) is a symmetrical process with a key length of 128 bits. CAST permits the modification of parts of the algorithm at runtime.

- **Blowfish**

This development by the renowned cryptographer Bruce Schneier is a symmetrical encryption process. Blowfish achieves outstanding data throughput on multifunction processors. The process is reputed to be extremely efficient and secure. Blowfish is selected by default with a key length of 128 bits for *ELSA LANCOM VPN* by the LAN-LAN Wizard.



The encryption settings can be modified in the expert configuration under ELSA LANconfig. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers.

4.2.5

Key management—IKE

The **I**nternet **K**ey **E**xchange Protocol (IKE) permits the integration of subprotocols for managing the SAs and for key administration.

Within IKE, two subprotocols are used in *ELSA LANCOM VPN*: Oakley for the authentication of partners and key administration, and ISAKMP for managing the SAs.

Setting up the SAs with ISAKMP/Oakley

Each setup of an SA is performed in several steps (in the case of dynamic Internet connections, these steps are performed after the public IP address has been transferred):

- ① The initiator sends a plain-text message to the remote station via ISAKMP with the request to set up an SA and with proposals for the security parameters of the SA.
- ② The remote station replies with the acceptance of a proposal.
- ③ Both devices now generate key pairs, each consisting of a public and private key, for Diffie-Hellman encryption.
- ④ In two further messages, the devices exchange their public keys for Diffie-Hellman.
- ⑤ The further communication is encrypted with Diffie-Hellman. The initiator sends a hash value of his Shared Secret. The remote station verifies the hash value and replies with the hash value of its own Shared Secret. An

encrypted connection in which both partners have authenticated themselves exists as of this point. Phase 1 of the SA setup is thus completed.

- ⑥ In Phase 2, the session keys for the authentication and symmetrical encryption of the actual data transfer are generated at random and transferred.



Symmetrical processes are used for the encryption of the actual data transfer. Asymmetrical processes (also known as public-key encryption) are more secure as they do not require the exchange of secret keys. However, they require considerable processing resources and are thus significantly slower than symmetrical processes. In practice, public-key encryption is generally only used for the exchange of key material. The actual data encryption is then performed using the fast symmetrical process.

The regular exchange of new keys

ISAKMP ensures that new key material is regularly exchanged between the two devices during the SA. This takes place automatically and can be checked using the 'Lifetime' setting in the advanced configuration of *ELSA LANconfig*.

