

Remote Maintenance with WinCC flexible Communication via a Wide Area Network (WAN)

Virtual Private Network

Issue 12/04

Foreword

This document describes the connection between two local area networks (LAN) on the basis of a virtual private network (VPN).

It also explains the IPSec protocol. IPSec is a protocol that can be used to establish a secure IP connection.

Disclaimer / Liability

Siemens AG accepts no liability, regardless of the legal grounds, for damages arising from the use of this entry, apart from the statutory liability accepted, for example, for damage to items used for personal purposes, personal accidents or due to malicious intent or gross negligence.

Warranty

The entries relate to selected suggested solutions for queries with complex tasks which have been dealt with in Customer Support. We also wish to point out that current technology not does permit us to exclude the possibility of errors in software programs taking all application conditions into account. The entries have been compiled to the best of our knowledge. We cannot agree to accept any liability over and beyond the standard warranty for class C software in accordance with our "General Terms and Conditions for the Transfer of Software Products for Automation and Drive Technology". The programs are available on the Internet under individual licenses. They are non-transferable.

Contents

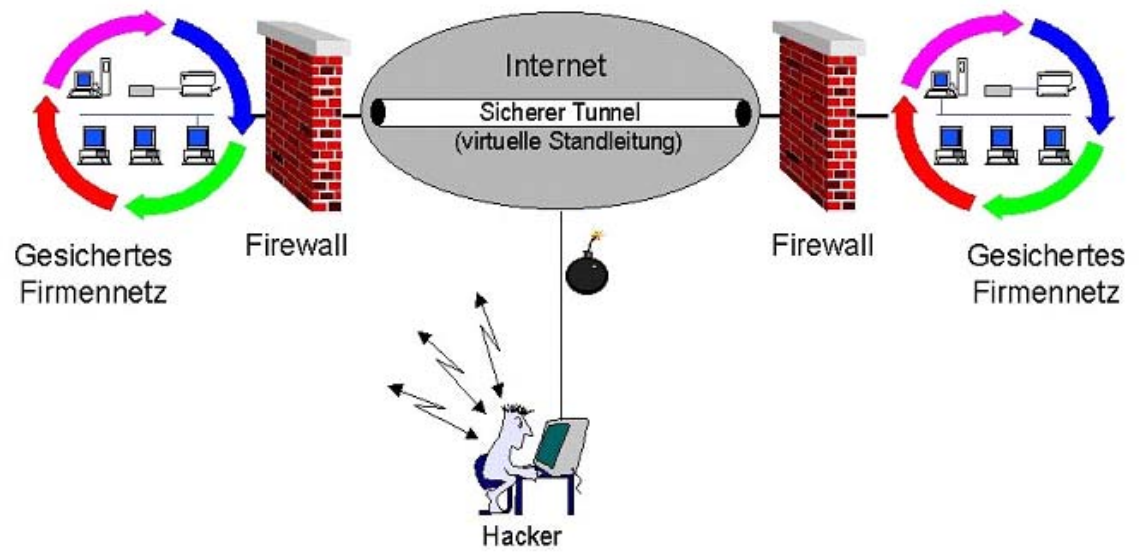
1	Virtual Private Network (VPN).....	5
1.1	Overview	5
1.2	Introduction	6
1.2.1	VPN-based connection between two LANs	6
2	Virtual Private Network with IPSec Protocol.....	7
2.1	Introduction	7
2.2	Communication via IPSec.....	8
2.3	Setting IPSec	8
2.3.1	Generating a license key	9
2.3.2	Setting up VPN the setup tool.....	11
2.3.3	Internet Key Exchange	16
2.3.4	Creating the PC-Client peer connection	24
2.4	Setting up the IPSec client on the PC.....	31
2.4.1	Installation of the client software.....	31
2.5	Testing the newly created connection:	43
3	Glossary	48
4	Warranty and Support	52

1 Virtual Private Network (VPN)

1.1 Overview

Fig.

1-1



1.2 Introduction

1.2.1 VPN-based connection between two LANs

Secure communication connections are advisable in high-security requirements to prevent machine data getting into the wrong hands.

The router offers a number of encryption systems for this purpose, which are combined under the generic term Virtual Private Network (VPN). When purchasing a router, ensure that it supports encryption in both directions. Local --> external and external --> local.

The PPTP (Point-to-Point Tunneling Protocol) and the more recent IPSec (Internet Protocol Security) protocol are well established.

This encryption allows you to establish a connection between two routers which is protected externally and which enables you to contact all subscribers internally by name or via the local IP address.

Following the configuration of the VPN IPSec tunnel, handling is precisely as if you had a crossed network cable between your nodes.

The dialogs below give you a step-by-step guide to protecting your network against outside interference.

2 Virtual Private Network with IPSec Protocol

2.1 Introduction

IPSec is a protocol that can be used to establish a secure IP connection.

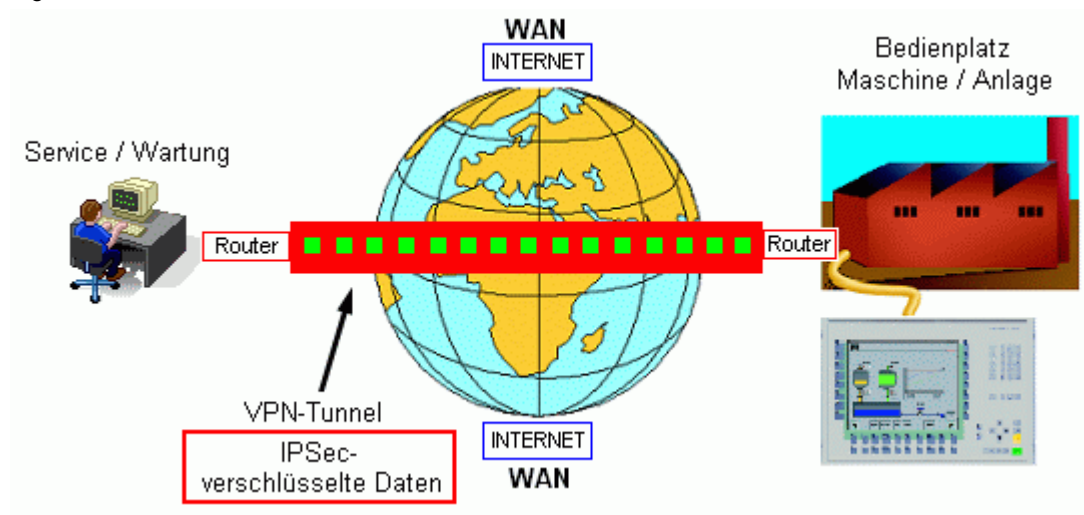
Refer to the following documents for the basic router configuration for communication via ISDN / DSL.

- Operator panel in communication with a router via ISDN
- Operator panel in communication with a router via DSL

Data security is guaranteed via the 4 functions below:

- Encryption (by means of ESP = Encapsulation Security Payload)
- Message integrity (ensuring that the message has not been changed)
- Sender authentication
- Key management.

Fig. 2-1



2.2 Communication via IPSec

Anwendung

Use IPSec to create a connection between two routers, as well as external Internet computers.

The encryption gives rise to a virtual tunnel (VPN tunnel) between the routers. You can work within the networks as if you were in a local network.

Once the network has been established, all the messages are assigned an additional header for the purposes of encryption.

A VPN IPSec connection is always recommended if you wish to prevent third parties from accessing your network.

2.3 Setting IPSec

The IPSec dialogs can only be displayed on your computer if you enter the license key via the setup tool first.

When you purchase the router, it will generally come with an IPSec license.

You are given three numbers for this license:

- Type of license
- License serial number
- PIN code

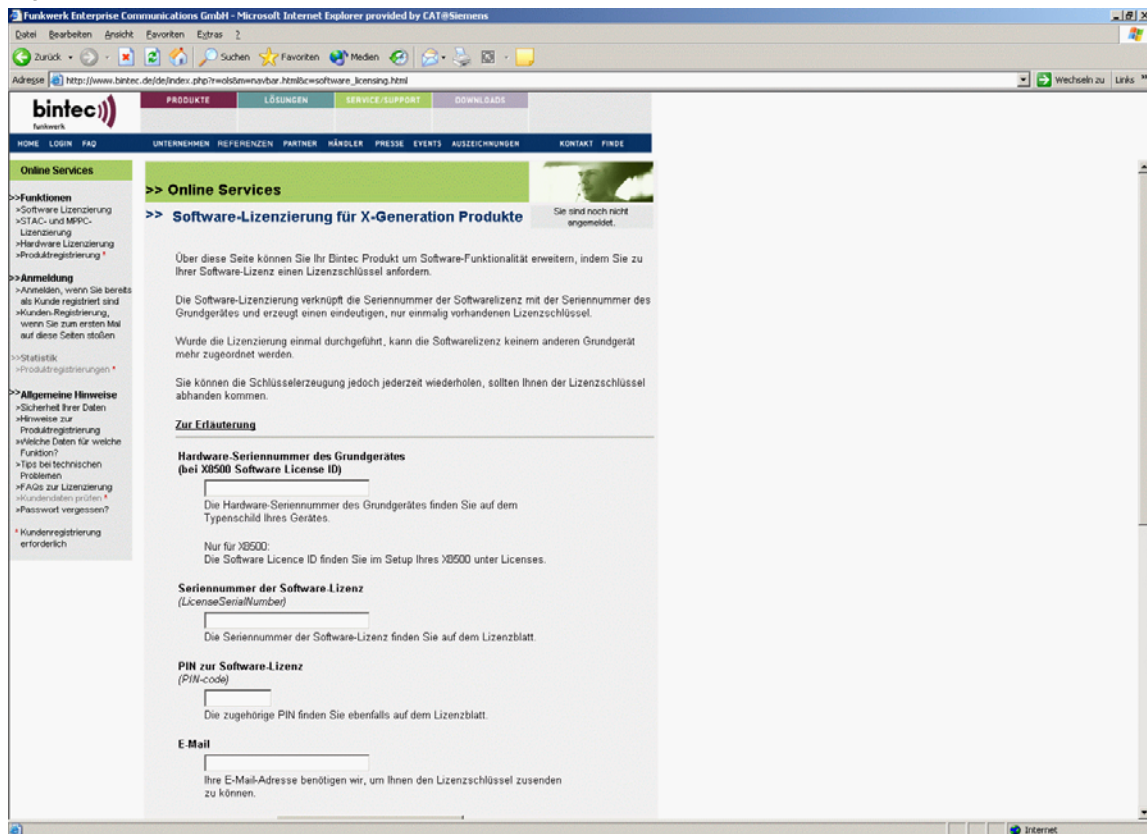
You will need the license serial number and PIN code in order to generate the license key on the BinTec website.

Go to the BinTec website at www.bintec.de via the Internet Explorer.

2.3.1 Generating a license key

On the BinTec home page, click the Service/Support tab. You will find the entry **Online Services** there. Click on **Licensing** under it. You are now on the page shown below. You can enter the data requested. This procedure may be different for each manufacturer.

Fig. 2-2



You can also extend the software functionality of your BinTec product via this page by requesting a license key for your BinTec product.

Software licensing links the serial number of the software license to the serial number of the base unit, generating a unique, unrepeated license key. Once the licensing has been performed, the software license cannot be assigned to any other base unit. However, you can generate another key any time if you mislay your license key.

You require the following for software licensing:

- The hardware serial number of the base unit which you can find on your device's rating plate or, in the case of the X8500, the software license ID from the setup menu
- The serial number of the software license
- The PIN for your protection in order to ensure that the license purchased by you is also assigned to you, e.g. for support. You receive the PIN along with the serial number of the software license.

You are shown the license key on the website. In addition, you also receive notification by e-mail from BinTec.

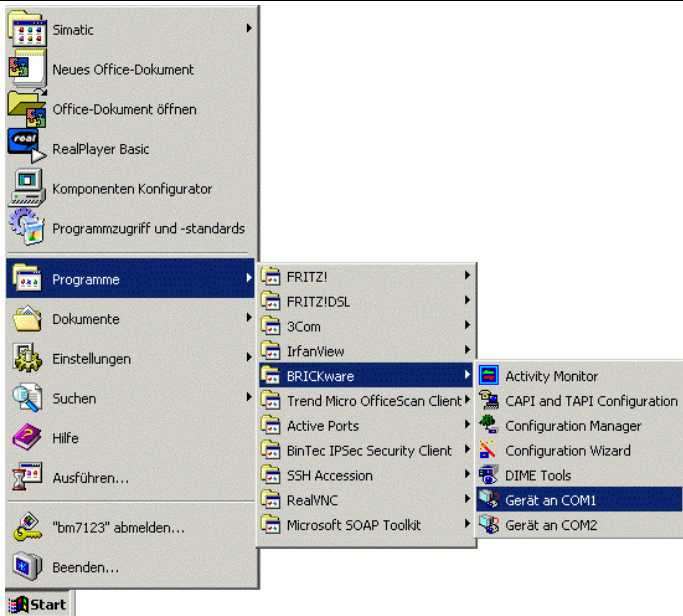
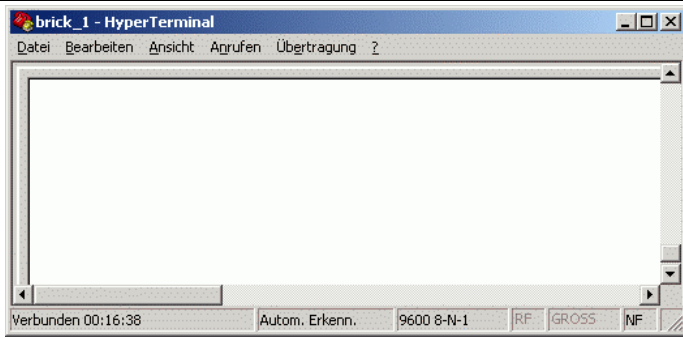
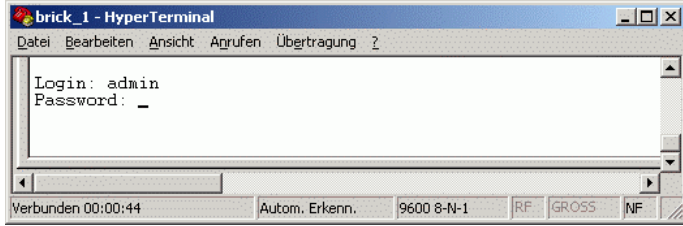
This key is now configured in your router in order to enable the software functionality.

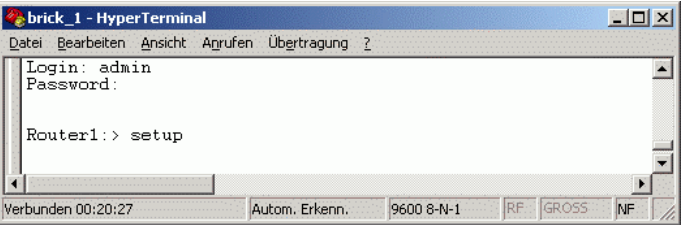
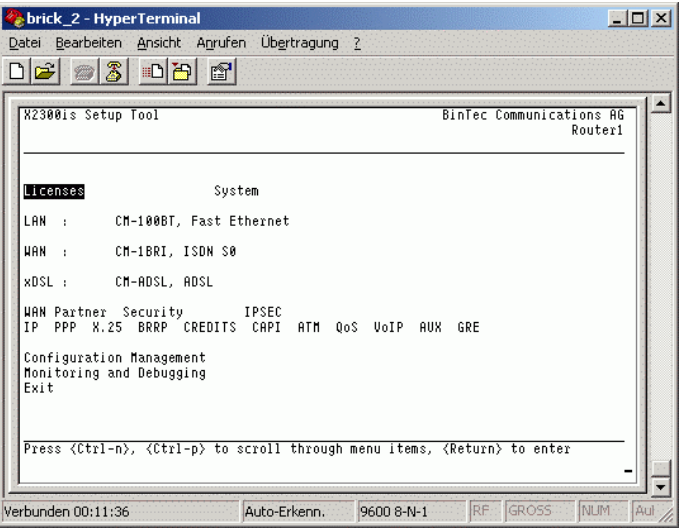
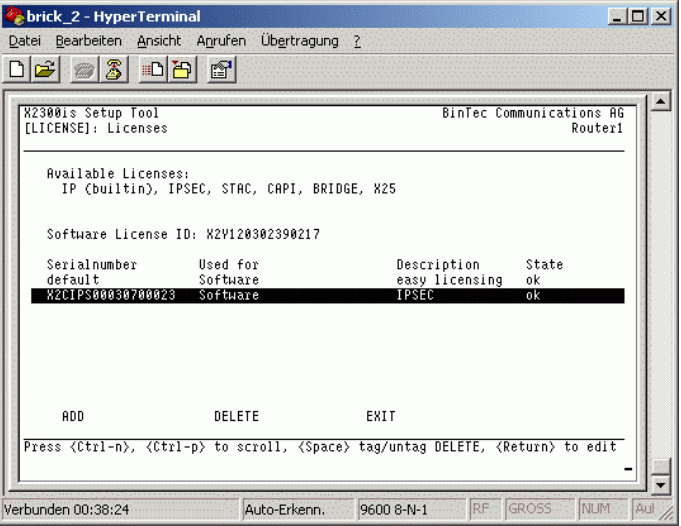
BinTec's FAQs contain information about this.

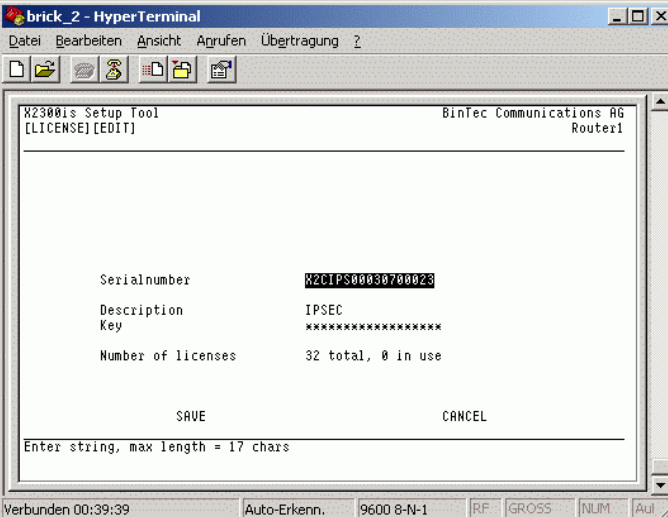
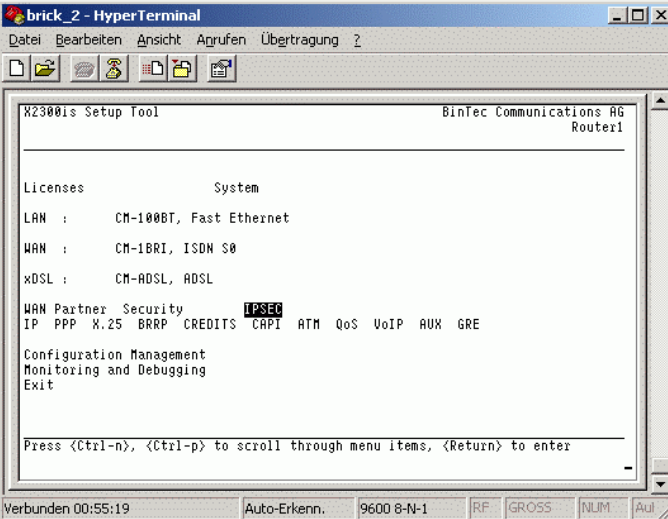
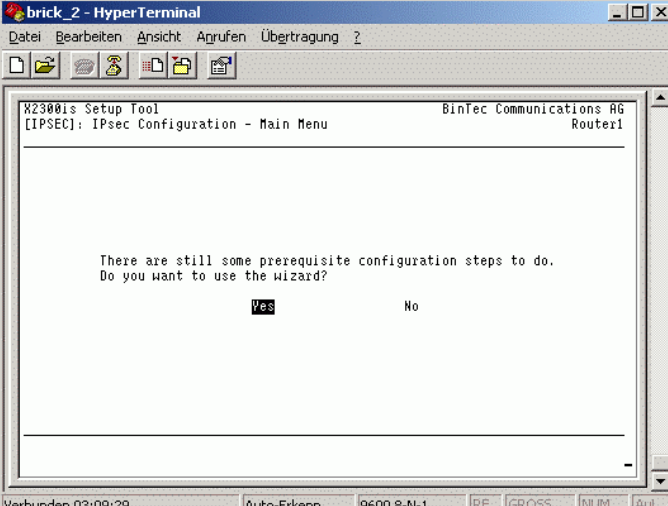
In order to enter the license key, start the BinTec setup tool once again and open the **Licenses** menu.

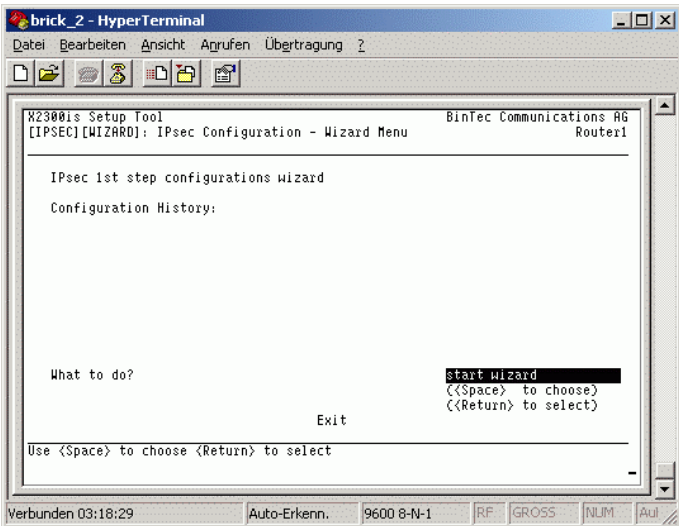
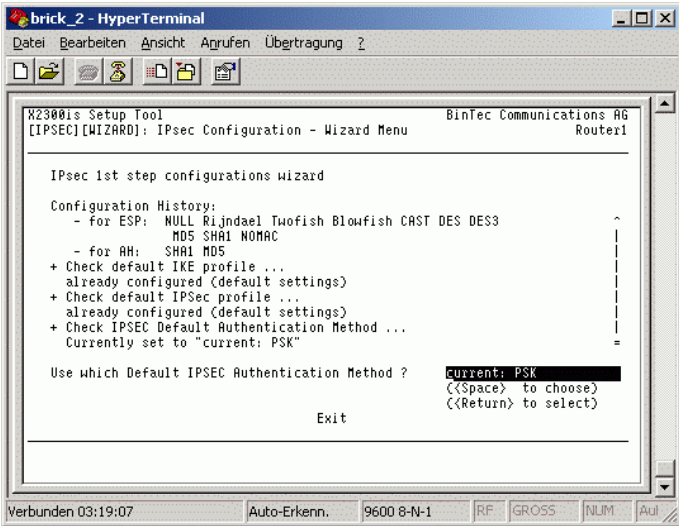
2.3.2 Setting up VPN the setup tool

Table 2-1

No.	Action	Note
1	<p>The BRICKware from BinTec that is already installed contains two default connections to your router. Depending on the COM port being used, now select a connection; the Windows HyperTerminal opens.</p> <p>Start > Programs > BRICKware > Device at COM1</p>	
2	<p>HyperTerminal</p> <p>Press ENTER to continue.</p>	
3	<p>After you press Enter to confirm, a login prompt appears in which you enter the user data that is defined in your basic configuration. Enter admin as the login, for example, followed by Enter and then the relevant password.</p>	

No.	Action	Note
4	Following login, enter setup ; this takes you to the setup tool.	
5	Setup tool. Open the Licenses menu.	
6	This takes you straight to a default license where you can now enter your IPsec key numbers via the ADD option.	

No.	Action	Note
7	<p>Enter the serial number and the key which is generated in the website in order to enable the IPSec functions.</p> <p>Click Save to close the dialog and go back to the main menu.</p>	
8	<p>A new option, IPSEC, now appears in your main menu. Start IPSec.</p>	
9	<p>Use the wizard to define the basic settings for your VPN IPSec connections in your company network.</p> <p>Click Yes to confirm.</p>	

No.	Action	Note
10	Select start wizard here.	 <p> start wizard ((\$space) to choose) ((\$Return) to select) </p>
11	<p>First of all select which authentication method you wish to use.</p> <p>PSK (pre-shared key) has been selected in this example.</p> <p>As a result of this process, the same key data is entered for both connection partners, enabling identification to take place..</p>	 <p> current: PSK ((\$space) to choose) ((\$Return) to select) </p>

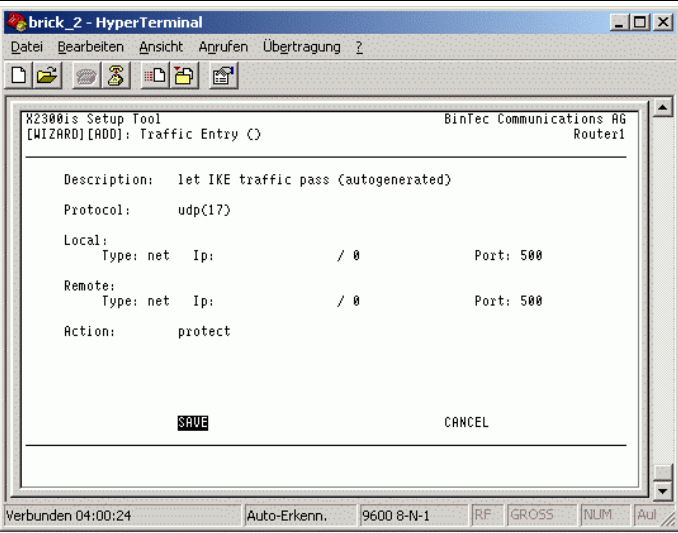
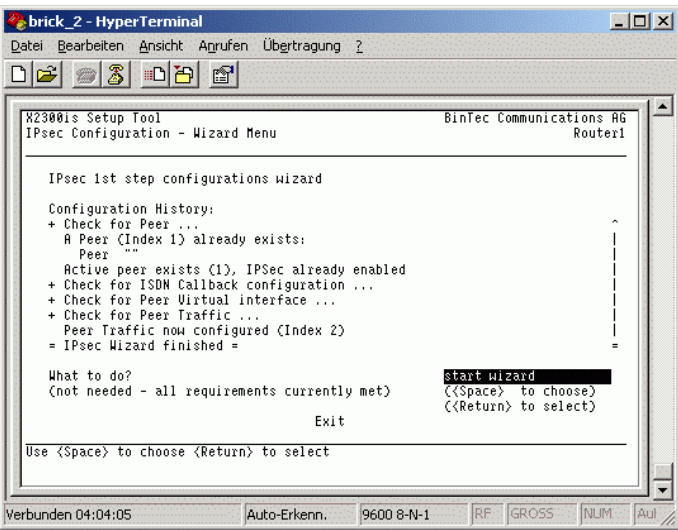
12	<p>Following this selection, a default route has to be created on the router via UDP protocol Port 500; the key data can be exchanged and compared between the routers via this route.</p> <p>Note: UDP is short for User Datagram Protocol, the name of a transmission protocol. It can be used on the basis of the IP protocol instead of the TCP. UDP does function on a connection-oriented basis. This means that a UDP data package can also be sent without an existing connection.</p>
13	<p>Select Start and press Enter to confirm. After start, define the settings listed in the table as follows.</p> <p>The description is user-definable and should be named to reflect the functionality of the connection. The default route enables the routers or PC clients to exchange connection parameters via the IKE.</p> <div data-bbox="683 689 1369 1205"> </div>

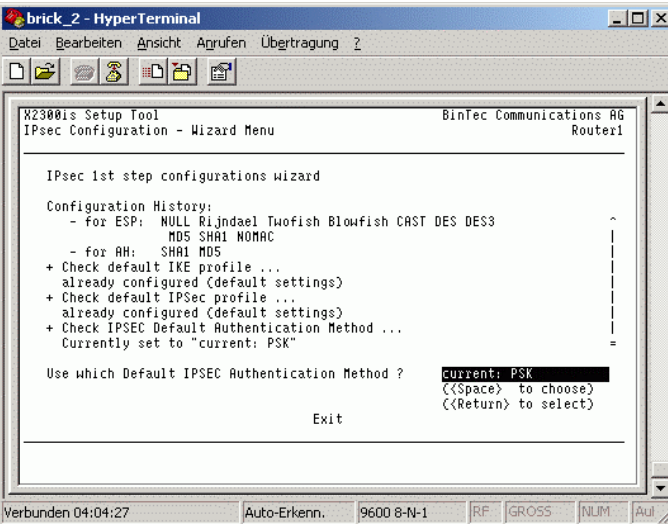
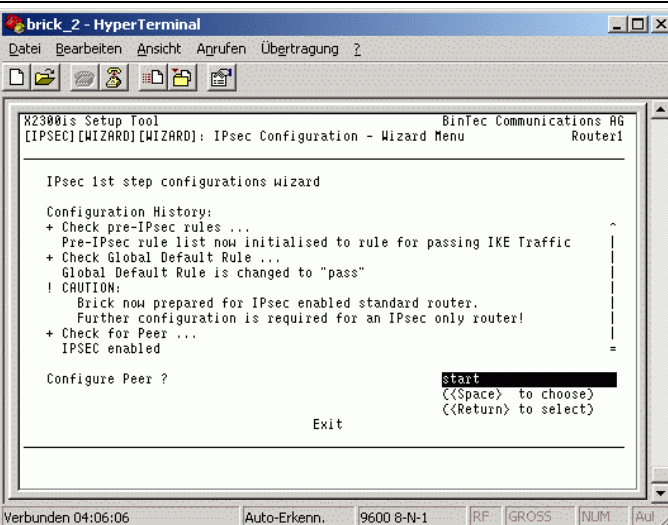
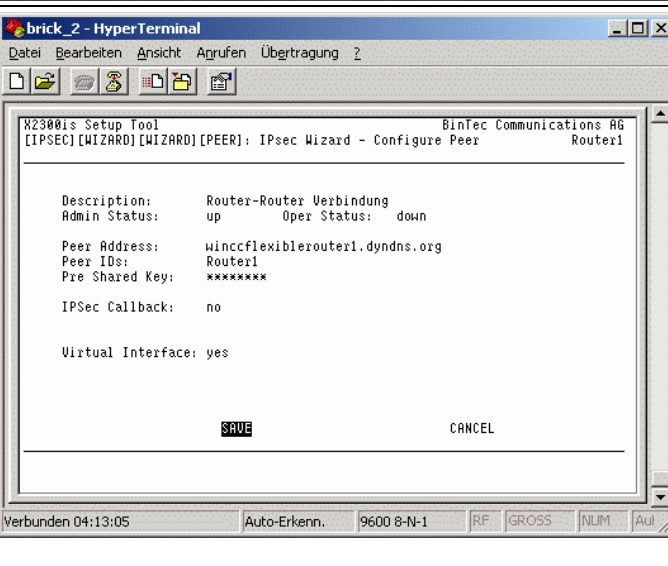
2.3.3 Internet Key Exchange

Internet Key Exchange (IKE) is a protocol that is used to manage security associations within VPN connections that are created with IPSec.

IKE is used because IPSec does not transmit the information which is required for encryption itself (algorithms, keys, period of validity, etc.), it takes it from a local SAD (Security Association Database table of all the security associations which are active on a computer which belongs to a VPN in accordance with IPSec guidelines.)

Table 2-2

No.	Action	Note
14	Click SAVE to confirm the entry and continue with the wizard.	
15	Switch over to Start wizard to set up the individual routes to your network subscribers.	

16	<p>Now select the encryption again via Current: PSK (pre-shared key).</p>	 <p>brick_2 - HyperTerminal</p> <p>File Bearbeiten Ansicht Anrufen Übertragung ?</p> <p>X2300is Setup Tool BinTec Communications AG IPsec Configuration - Wizard Menu Router1</p> <p>IPsec 1st step configurations wizard</p> <p>Configuration History:</p> <ul style="list-style-type: none"> - for ESP: NULL Rijndael Twofish Blowfish CAST DES DES3 - for AH: SHA1 MD5 <p>+ Check default IKE profile ... already configured (default settings)</p> <p>+ Check default IPsec profile ... already configured (default settings)</p> <p>+ Check IPSEC Default Authentication Method ... Currently set to "current: PSK"</p> <p>Use which Default IPSEC Authentication Method ? current: PSK <<Space> to choose <<Return> to select</p> <p>Exit</p> <p>Verbunden 04:04:27 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>
17	<p>The configuration for the first peer starts.</p> <p>Select Start and press Enter to confirm.</p>	 <p>brick_2 - HyperTerminal</p> <p>File Bearbeiten Ansicht Anrufen Übertragung ?</p> <p>X2300is Setup Tool BinTec Communications AG [IPSEC] [WIZARD] [WIZARD]: IPsec Configuration - Wizard Menu Router1</p> <p>IPsec 1st step configurations wizard</p> <p>Configuration History:</p> <ul style="list-style-type: none"> + Check pre-IPsec rules ... Pre-IPsec rule list now initialised to rule for passing IKE Traffic + Check Global Default Rule ... Global Default Rule is changed to "pass" <p>! CAUTION: Brick now prepared for IPsec enabled standard router. Further configuration is required for an IPsec only router!</p> <p>+ Check for Peer ... IPSEC enabled</p> <p>Configure Peer ? start <<Space> to choose <<Return> to select</p> <p>Exit</p> <p>Verbunden 04:06:06 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>
18	<p>The settings shown here also need to be entered for the peer.</p> <p>Only the Peer Address and Peer ID differ.</p>	 <p>brick_2 - HyperTerminal</p> <p>File Bearbeiten Ansicht Anrufen Übertragung ?</p> <p>X2300is Setup Tool BinTec Communications AG [IPSEC] [WIZARD] [WIZARD] [PEER]: IPsec Wizard - Configure Peer Router1</p> <p>Description: Router-Router Verbindung Admin Status: up Oper Status: down</p> <p>Peer Address: winccflexiblerouter1.dyndns.org Peer IDs: Router1 Pre Shared Key: *****</p> <p>IPSec Callback: no</p> <p>Virtual Interface: yes</p> <p>SAVE CANCEL</p> <p>Verbunden 04:13:05 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>

19 **Note:**

The parameters are user-definable and can generally comprise up to 50 characters.
Configure the router --> router connection first. To do this you require the following items of information:

- Peer's name on the Internet if the IP address is always dynamic as is the case in our example (Peer Address)
- The peer's local name (Peer ID)
- The settings for the connection name (description) and pre-shared key must be identical in both subscribers.

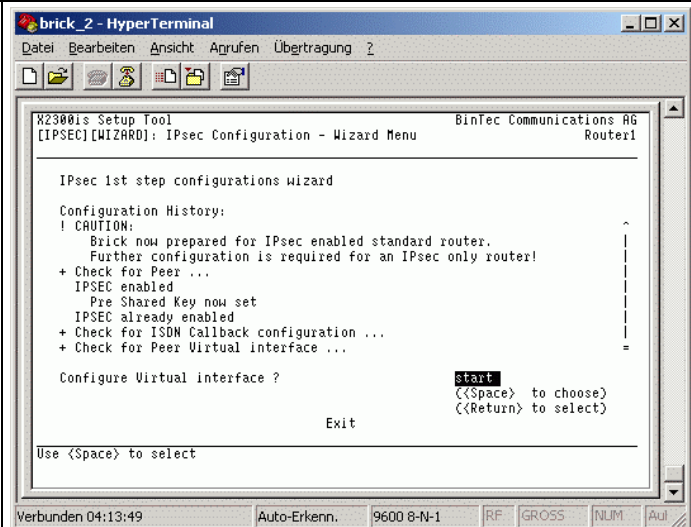
The pre-shared key (PSK) must be entered twice in a row in order to confirm the entry.

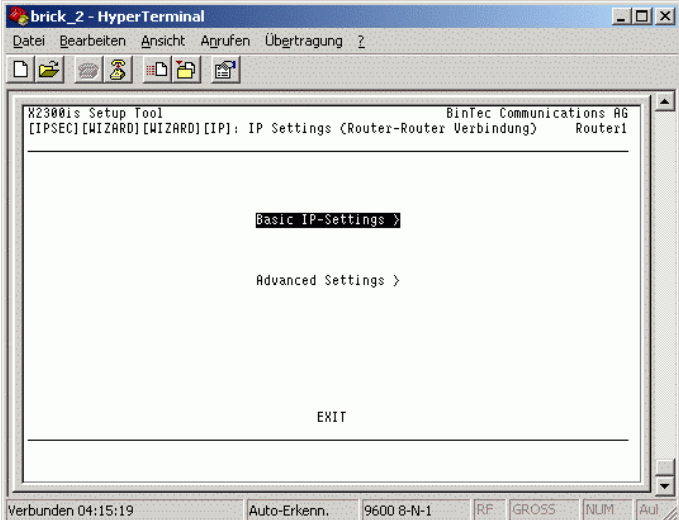
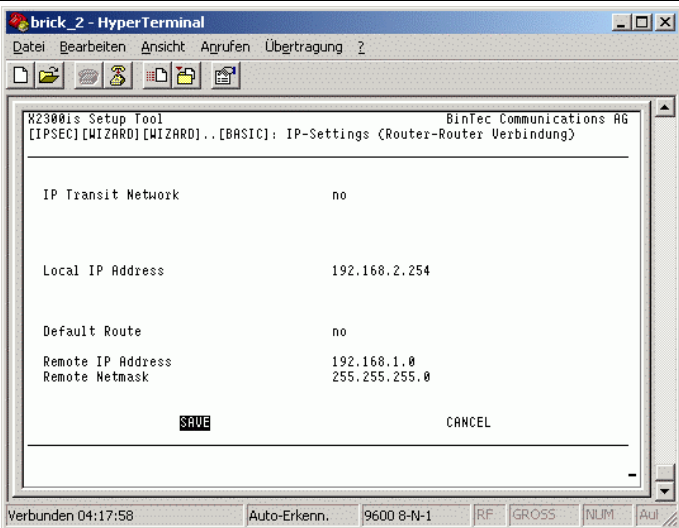
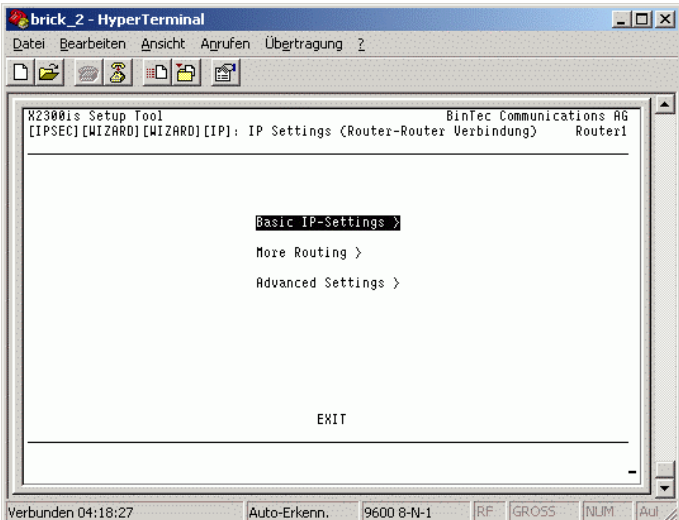
If you establish a connection between two routers, and your router supports ISDN and DSL connections at the same time, you can use the ISDN callback function.

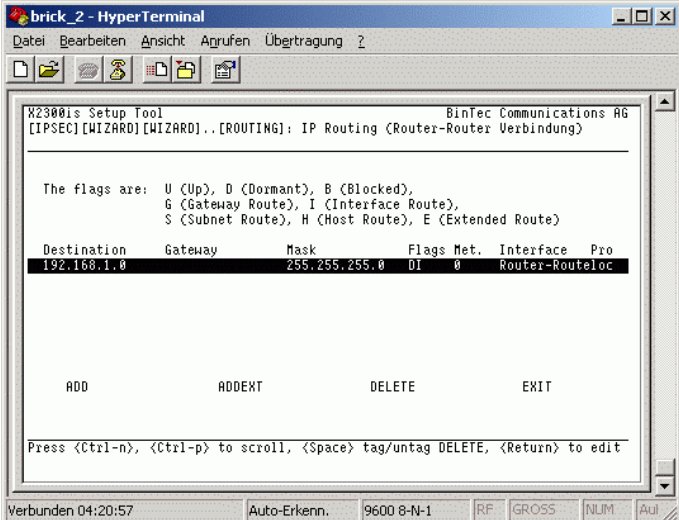
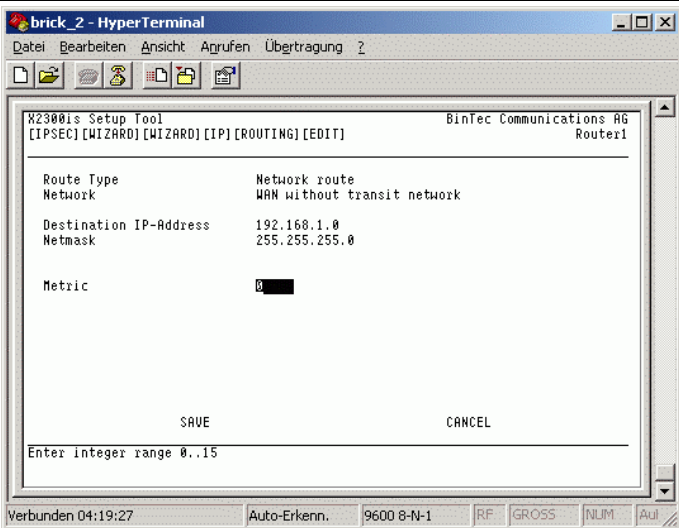
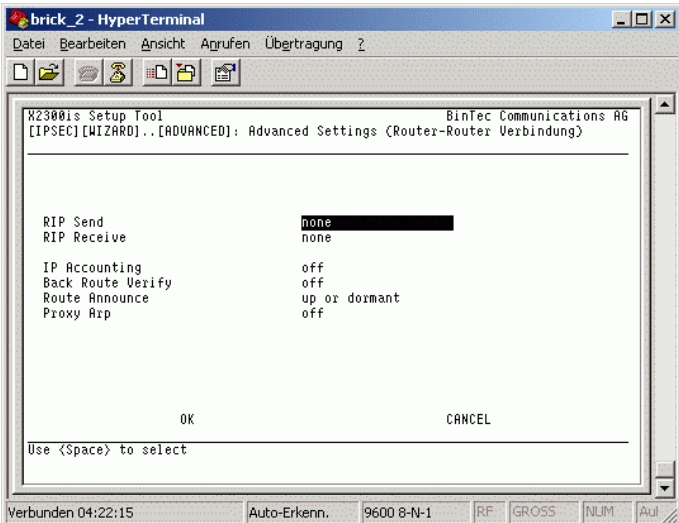
If the DSL line fails, this function provides a new IPSec tunnel via the ISDN line. This enhances the security for your data exchange.

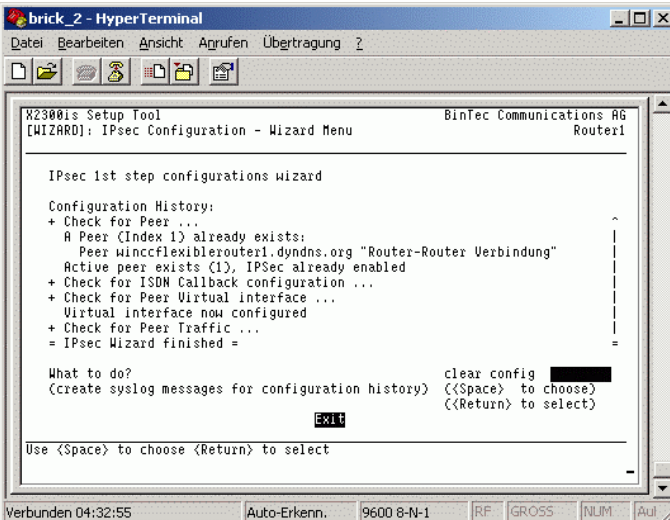
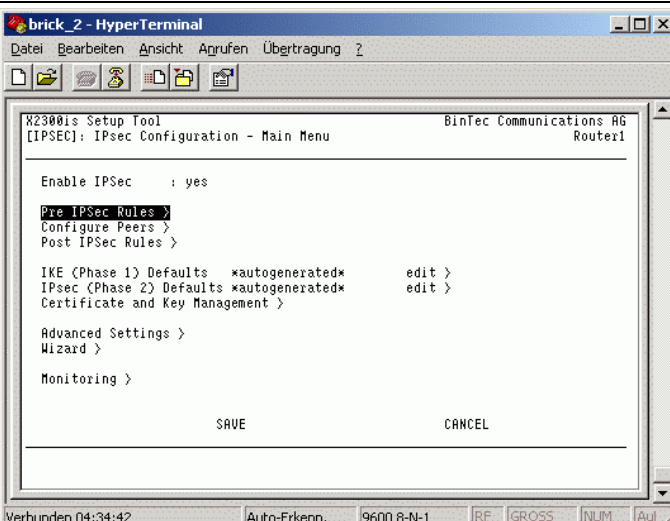
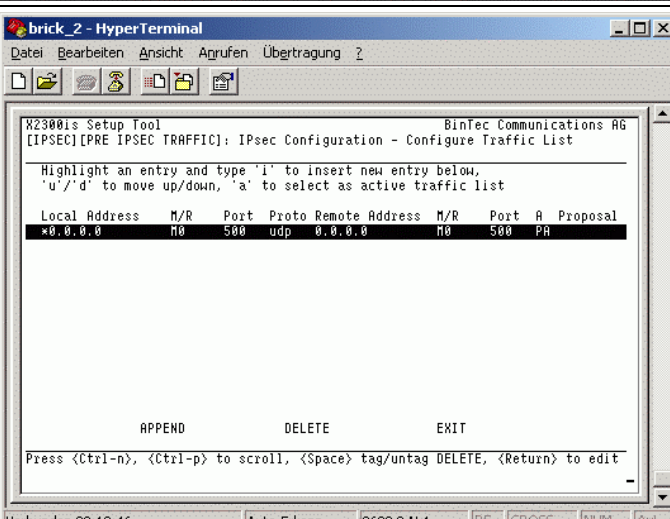
If you wish to use the callback, it must be enabled at either end.

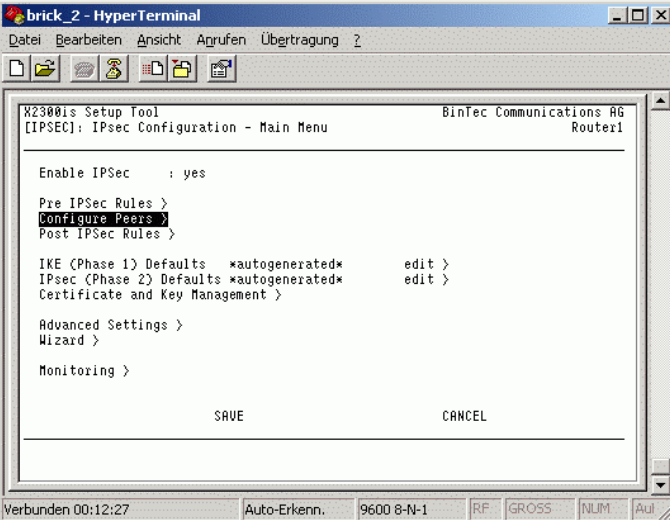
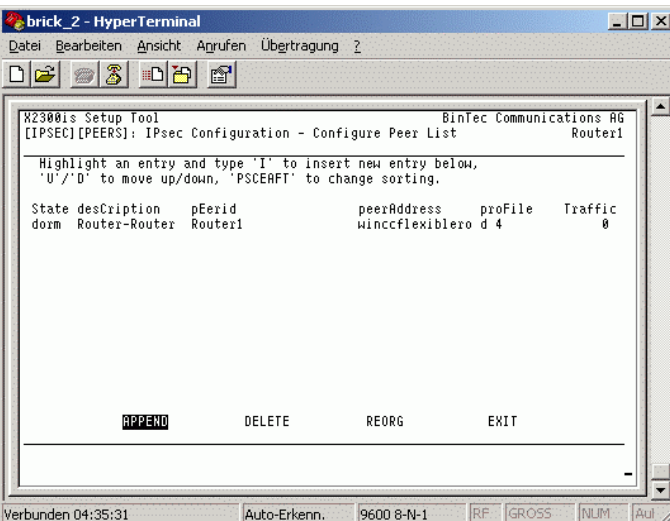
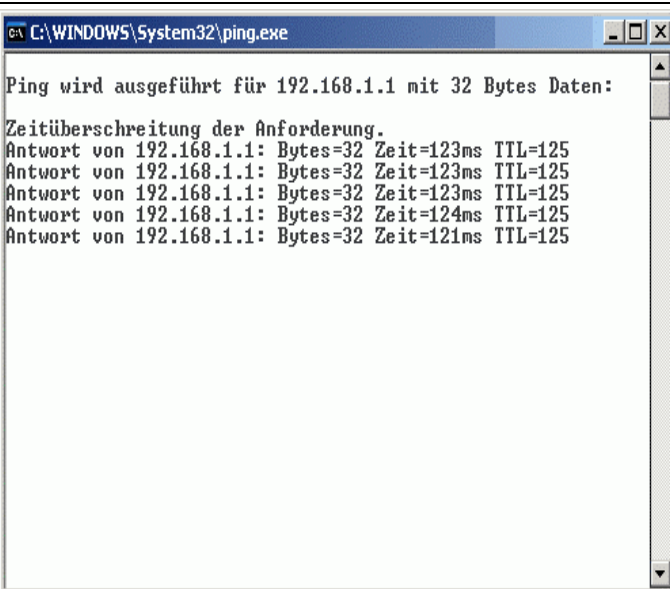
20 Some connection data relating to the peer network still has to be entered for the route which is currently being created.



21	Enter your peer network's data under Basic IP Settings .	
22	For this purpose you only require the starting address and the subnet mask. This enables the router to tell how big the peer network's IP band is.	
23	A route was created automatically as soon as this entry was made. You can check it once again under the menu option More Routing .	

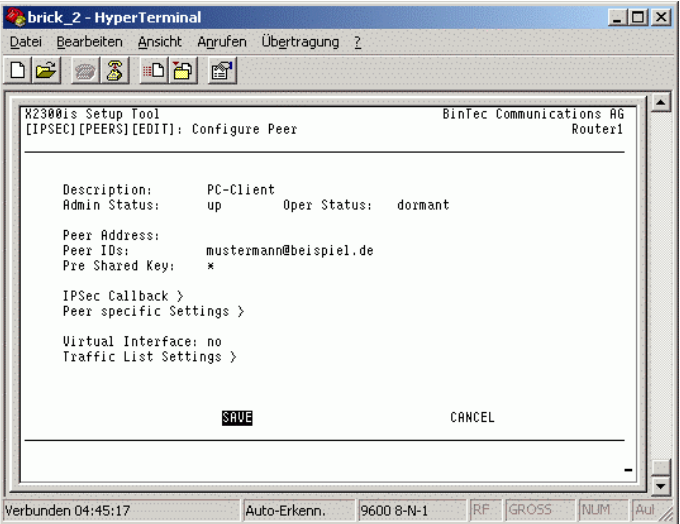
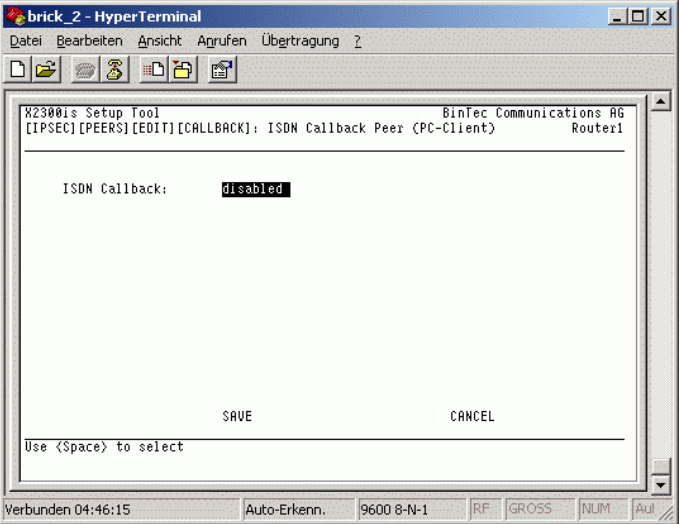
24	<p>Press ENTER to open the existing entry.</p>	
25	<p>If you have closed the dialog by clicking CANCEL, you can still process the Advanced Settings option. (-> See point 20)</p> <p>However, there has been no need to change the defaults at this point.</p>	
26	<p>This completes the basic configuration. Further connections can be created either directly in the menu or by restarting the wizard. The creation of the default route via UDP Port 500 does not take place yet.</p> <p>The connection between two networks is completed at this point.</p> <p>Click OK to continue.</p>	

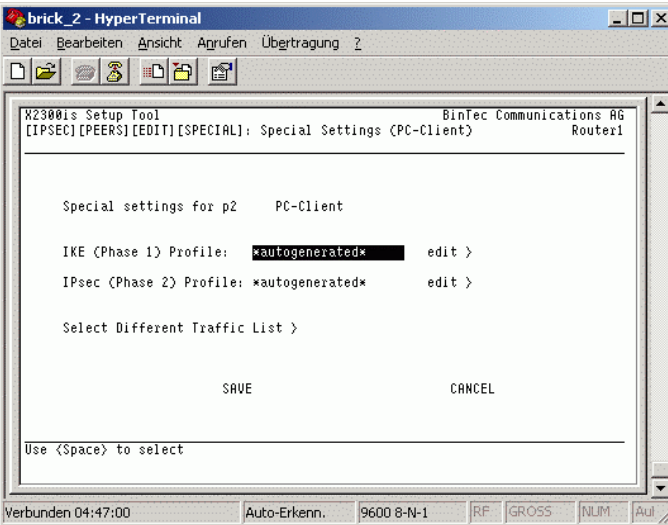
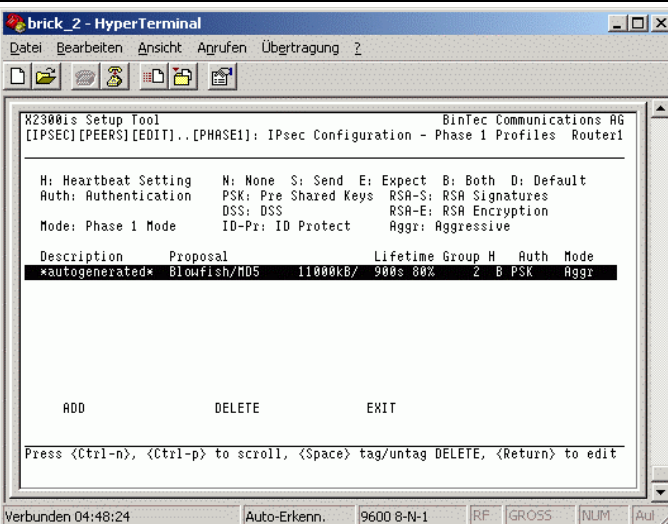
27	Click Exit to close the menu.	 <p>brick_2 - HyperTerminal</p> <p>BinTec Communications AG Router1</p> <p>X2300is Setup Tool [WIZARD]: IPsec Configuration - Wizard Menu</p> <p>IPsec 1st step configurations wizard</p> <p>Configuration History:</p> <ul style="list-style-type: none">+ Check for Peer ...<ul style="list-style-type: none">A Peer (Index 1) already exists: Peer winccflexiblerouter1.dyndns.org "Router-Router Verbindung"+ Active peer exists (1), IPsec already enabled+ Check for ISDN Callback configuration ...+ Check for Peer Virtual interface ...<ul style="list-style-type: none">Virtual interface now configured+ Check for Peer Traffic ...= IPsec Wizard finished = <p>What to do? (create syslog messages for configuration history) clear config []</p> <p>Use <Space> to choose <Return> to select</p> <p>Exit</p> <p>Verbunden 04:32:55 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>																		
28	Under Pre IPSec Rules you can find the default route via UDP which you created with the wizard.	 <p>brick_2 - HyperTerminal</p> <p>BinTec Communications AG Router1</p> <p>X2300is Setup Tool [IPSEC]: IPsec Configuration - Main Menu</p> <p>Enable IPsec : yes</p> <p>Pre IPSec Rules ></p> <p>Configure Peers ></p> <p>Post IPsec Rules ></p> <p>IKE (Phase 1) Defaults *autogenerated* edit ></p> <p>IPsec (Phase 2) Defaults *autogenerated* edit ></p> <p>Certificate and Key Management ></p> <p>Advanced Settings ></p> <p>Wizard ></p> <p>Monitoring ></p> <p>SAVE CANCEL</p> <p>Verbunden 04:34:42 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>																		
29	Default Route	 <p>brick_2 - HyperTerminal</p> <p>BinTec Communications AG</p> <p>X2300is Setup Tool [IPSEC][PRE IPSEC TRAFFIC]: IPsec Configuration - Configure Traffic List</p> <p>Highlight an entry and type 'I' to insert new entry below, 'u'/'d' to move up/down, 'a' to select as active traffic list</p> <table><thead><tr><th>Local Address</th><th>M/R</th><th>Port</th><th>Proto</th><th>Remote Address</th><th>M/R</th><th>Port</th><th>A</th><th>Proposal</th></tr></thead><tbody><tr><td>*0.0.0.0</td><td>n0</td><td>500</td><td>udp</td><td>0.0.0.0</td><td>n0</td><td>500</td><td>PH</td><td></td></tr></tbody></table> <p>APPEND DELETE EXIT</p> <p>Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit</p> <p>Verbunden 00:10:46 Auto-Erkenn. 9600 8-N-1 RF GROSS NUM Aul</p>	Local Address	M/R	Port	Proto	Remote Address	M/R	Port	A	Proposal	*0.0.0.0	n0	500	udp	0.0.0.0	n0	500	PH	
Local Address	M/R	Port	Proto	Remote Address	M/R	Port	A	Proposal												
*0.0.0.0	n0	500	udp	0.0.0.0	n0	500	PH													

30	<p>In the Configure Peers menu option you specify all the connections which you require with peer networks.</p>	
31	<p>This menu already includes the connections that had previously been configured between your routers. Now add the PC-client connection in order to give your service personnel access to your local network.</p> <p>Click APPEND to create the new entry.</p> <p>Click EXIT to close the settings.</p>	
32	<p>Note:</p> <p>The settings must be configured identically on the second router.</p> <p>The connection between the routers can be tested quite simply by contacting a subscriber in the peer network from a subscriber on the local network, (e.g. ping).</p> <p>The routers then negotiate the IPSec tunnel; this then facilitates the sort of connection that exists within a closed network.</p> <p>The first time-out occurs because the tunnel has not been set up yet.</p>	

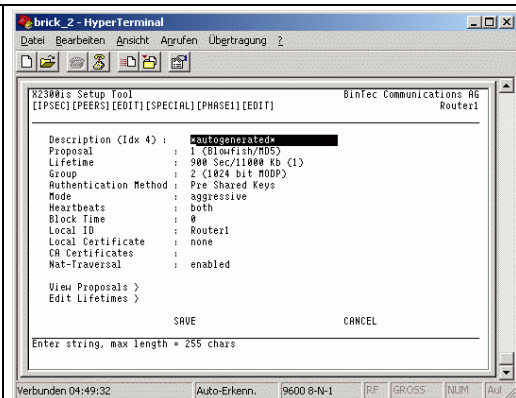
2.3.4 Creating the PC-Client peer connection

Table 2-3

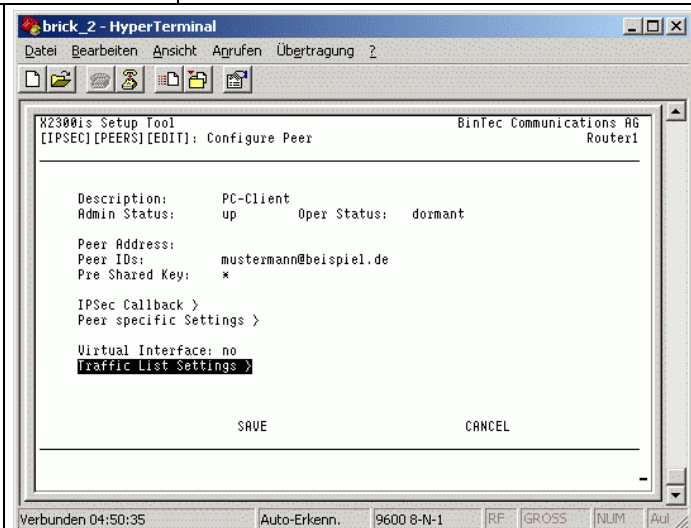
No.	Action	Note
33	<p>The name under Description is, once again, user-definable and has no bearing on encryption.</p> <p>The Peer Address entry is left blank in this case because the PC-client user generally does not have a permanent IP address and does not have a DynDNS account for its service PC on the Internet.</p> <p>We use an e-mail address as the Peer IDs (user name) because it has a long string of characters; however, you can choose any name.</p> <p>Both sides must always use the same parameters.</p> <p>The Pre Shared Key must be entered twice to ensure that it can be copied correctly.</p>	
34	<p>There is no need to enable the ISDN Callback, shown here, in the case of a PC-client connection because there is no callback function on the PC.</p>	

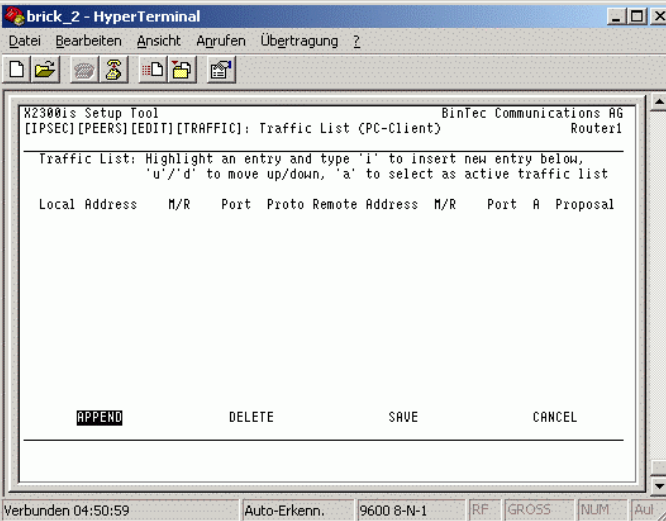
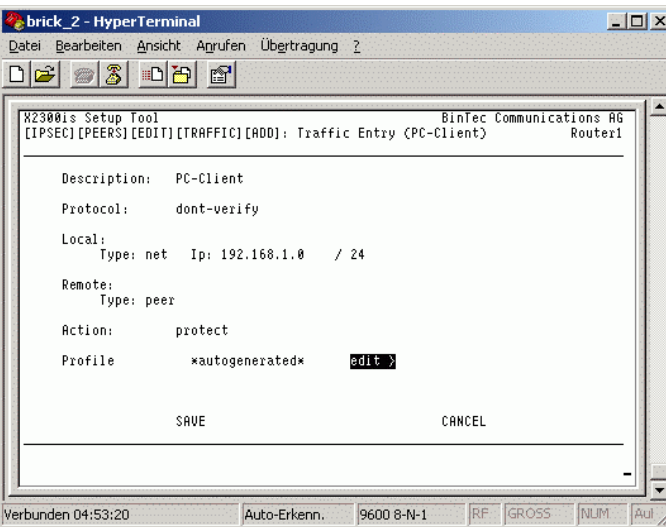
35	<p>The Peer-specific Settings menu option (figure 30) contains the settings for the 1st and 2nd identification phases. Use the autogenerated setting; thus, the router itself decides which encryption protocols to use. Click edit to open the settings because you must take a note of the settings on your PC-Client.</p>	
36	<p>Press ENTER to open the selected entry in order to take a note of the settings or to change them.</p>	

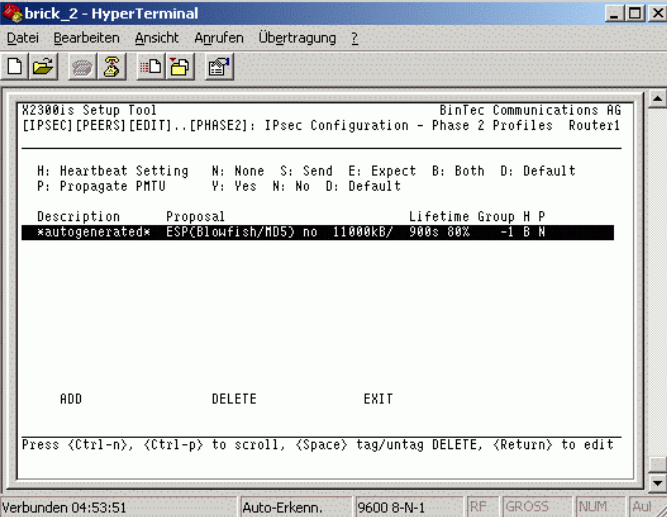
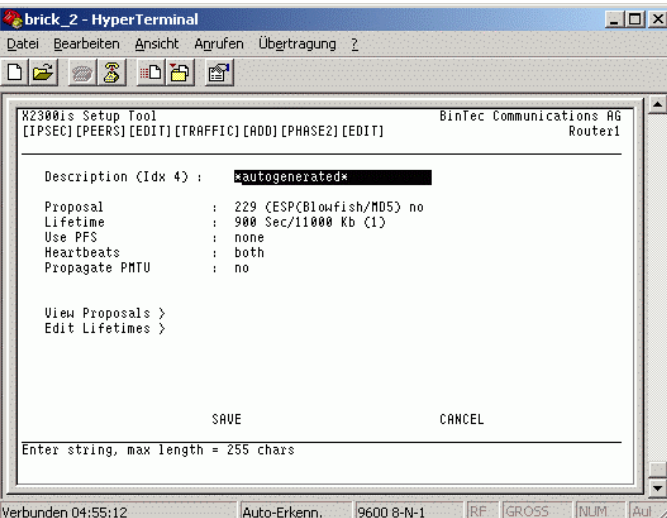
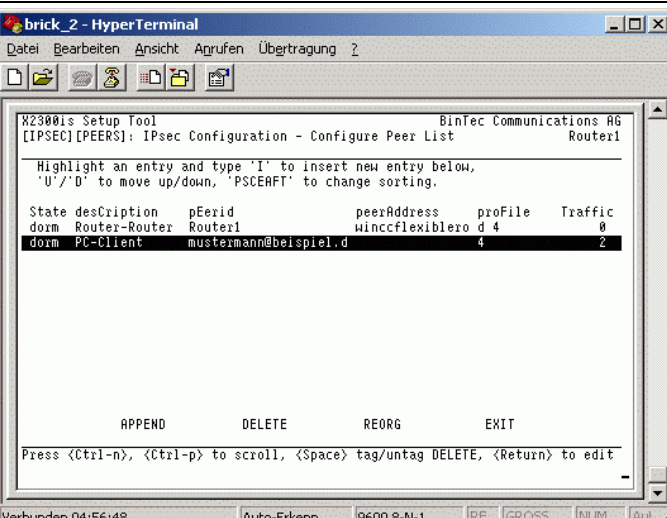
- 37 These are the default settings apart from Lifetime, which has been raised from default to 900 seconds.
The router now exchanges the initial data via the Blowfish algorithm.
The other algorithms MD5 and MODP are also used for encryption and contain the mechanisms that are used for authentication. Since your PC is generally assigned a dynamic IP address by the ISP, **Aggressive Mode** must be set on the router and on the client.
Set the **Authentication Method** to the **Pre Shared Keys** process selected by us. Use the **Heartbeats** settings to define whether the connection is to be controlled by only one of the subscribers or both. If there are no heartbeats shown, the tunnel can be disabled quickly by either side. **Block Time** prevents re-connection for a certain length of time if the keys have not matched.
The last few settings are not discussed in this FAQ as they relate to additional certification. **View Proposals** contains a list of all the algorithms that you can use.
The final point to mention is **Edit Lifetimes**. Here you can define your own times to suit your requirements.

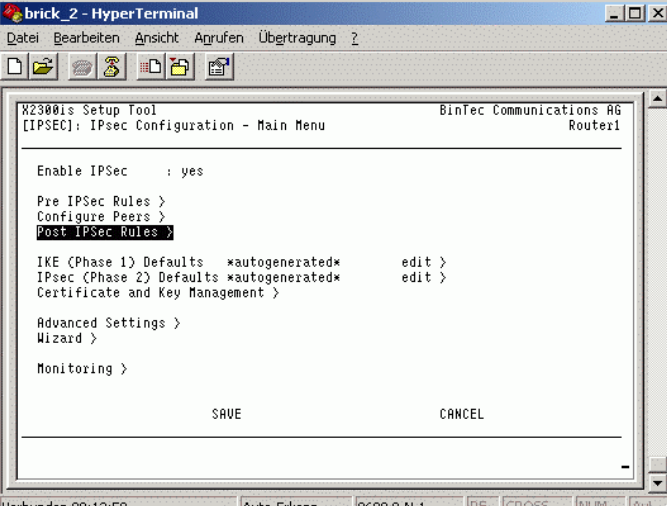
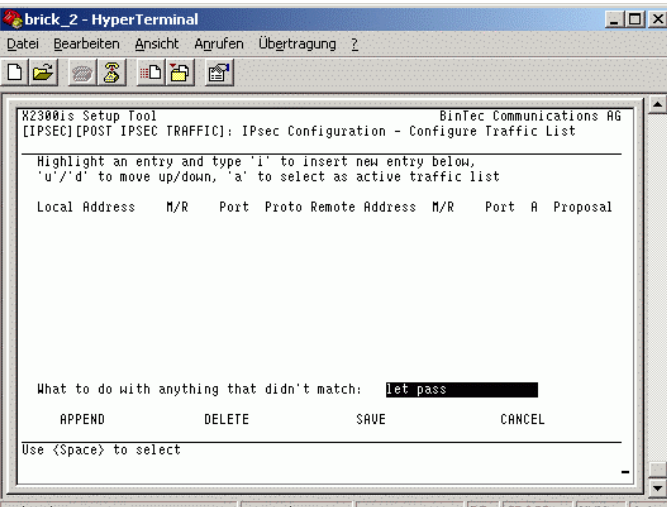
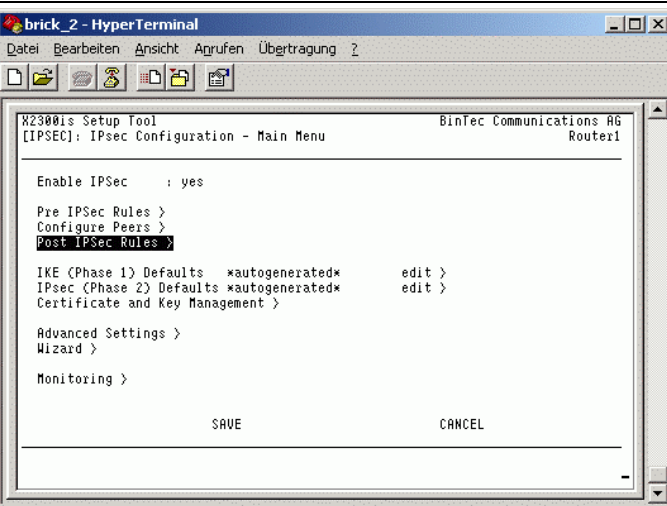


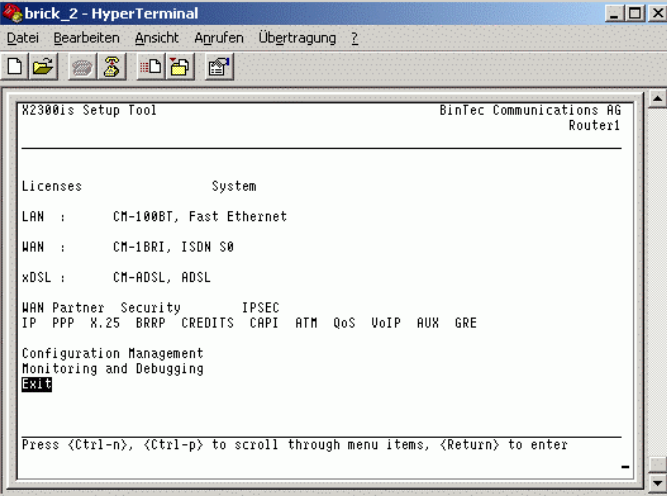
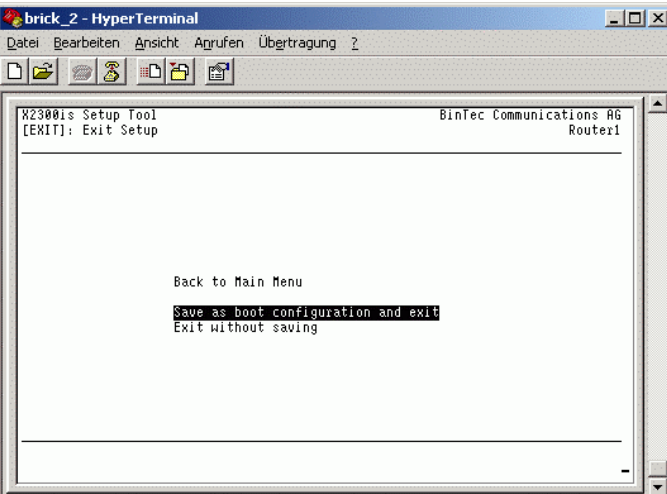
- 38 Once authentication of the IPSec tunnel is complete, you still need to define which parts of your network the peer may use.
For this purpose you require a **Traffic List** which can be created under the menu option of the same name.



39	<p>Click APPEND to add another new list.</p>	
40	<p>Complete network access has been allocated to enable the PC client to perform all the requisite steps during servicing.</p> <p>This gives rise to the settings shown.</p> <p>Do not select any special protocol, simply define all the IP addresses belonging to the local router network for the client.</p> <p>To facilitate this, specify the starting address.</p> <p>24 indicates that the subnet mask is using 24 bits. (255.255.255.0)</p> <p>The client's IP address is dynamic. By setting the Remote Type to peer, the router accepts the IP address, with which the client has logged in, as the network subscriber.</p> <p>Select EDIT under the Profile entry.</p>	

41	<p>Profile once again contains the settings for phase 2 which you know previously from the encryption of the first phase.</p> <p>Press Enter to open the entry</p>	
42	<p>After pressing Enter to confirm, the settings are listed</p>	
43	<p>Once you have closed the dialogs with SAVE, your PC-client connection is fully set up.</p> <p>Click EXIT to continue.</p>	

<p>44</p>	<p>In the Post IPSec Rules menu option, you must check whether the entry What to do with anything that didn't match is set to let pass. This means that anything that is not defined in the IPSec Rules is let through.</p> <p>Press Enter to continue.</p>	
<p>45</p>	<p>Check for let pass. This completes the configuration of IPSec. Click Save to go back and save the settings.</p>	
<p>46</p>	<p>You are now back in the main menu for the IPSec configuration.</p> <p>Click SAVE once again to exit the dialog.</p>	

47	Click EXIT to close the setup tool.	
48	Save everything once again as a boot configuration.	

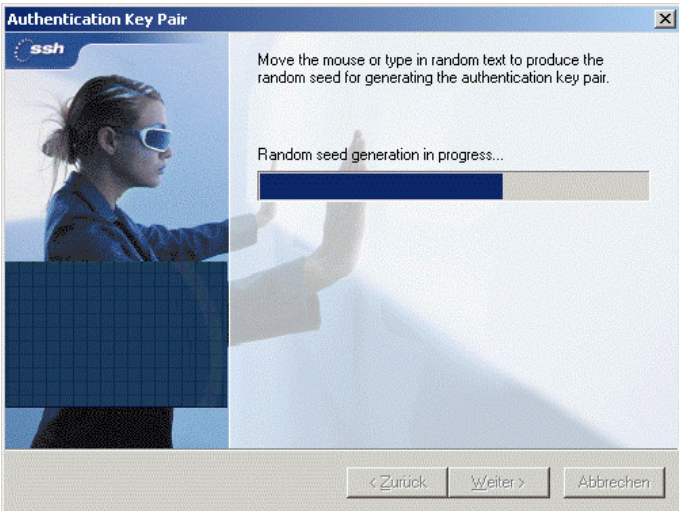
2.4 **Setting up the IPSec client on the PC.**

The setup takes place in our example on the basis of the SSH Sentinel PC client.
Whilst there are lots of other providers, the authentication and setting procedures are identical among almost all of them.
The installation steps described here represent an extension to an FAQ from BinTec.

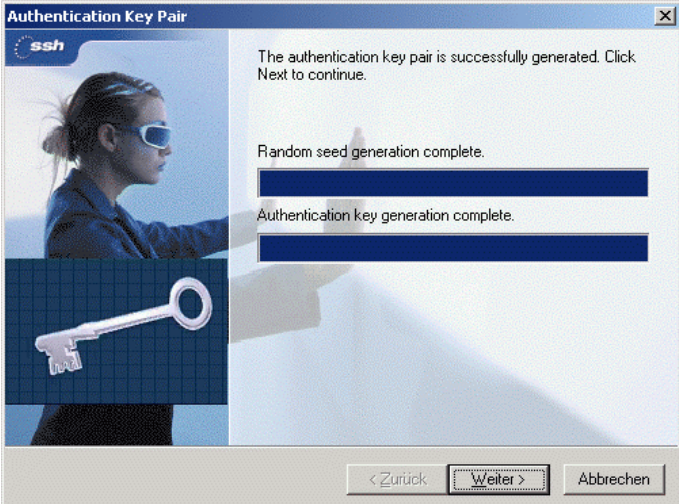
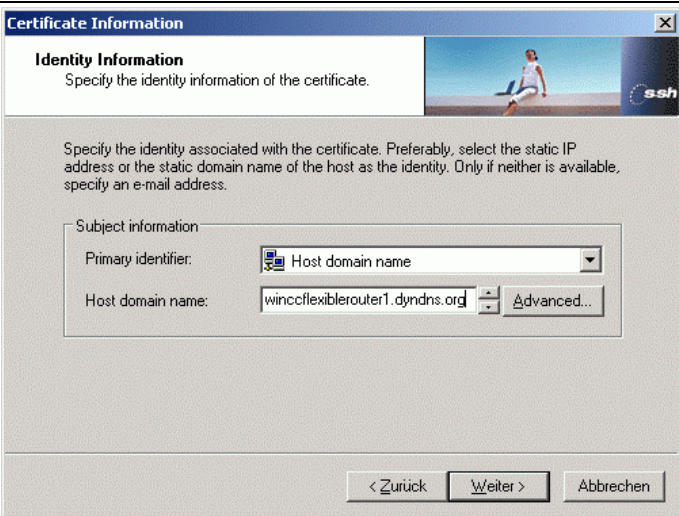
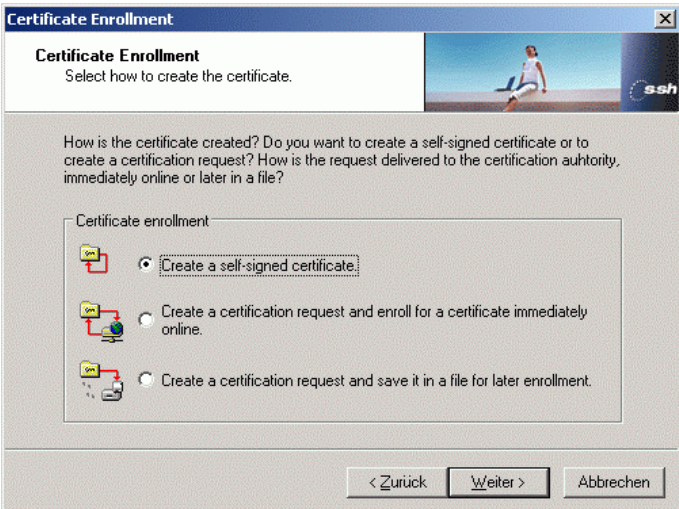
2.4.1 **Installation of the client software**

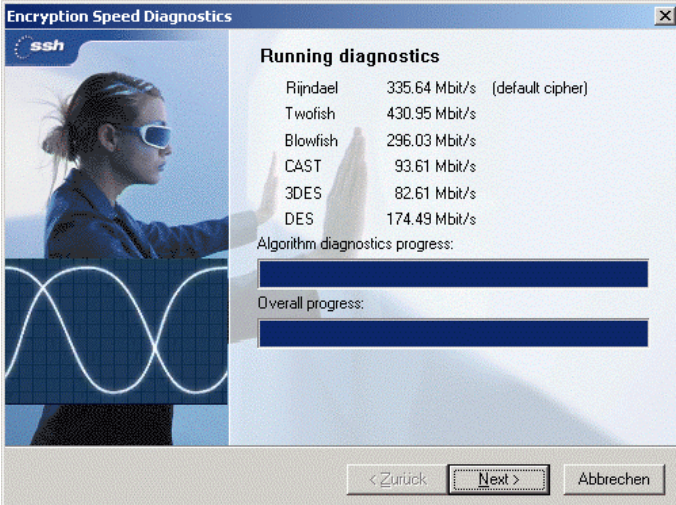
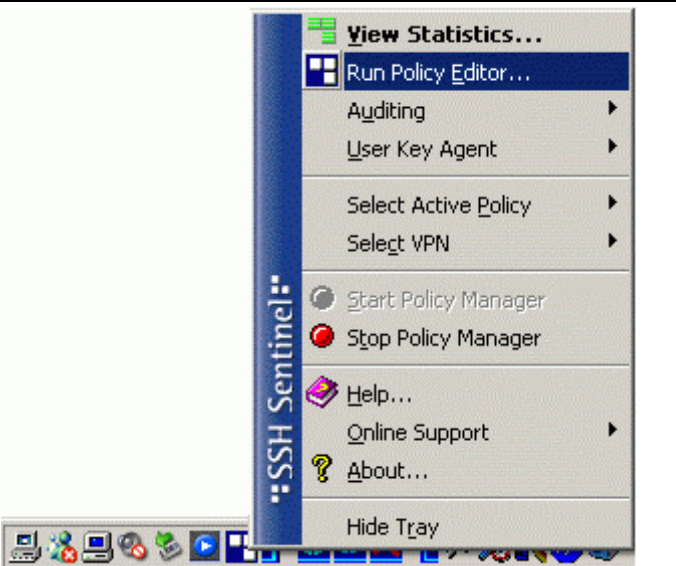
Simply start the installation via the setup function on the CD.
Note:
You can always find an up-to-date version of this in BinTec's downloads area.
Therefore, the dialogs may also deviate somewhat.
This document does not describe all the installation steps since many of them can be confirmed by simply clicking "Next".

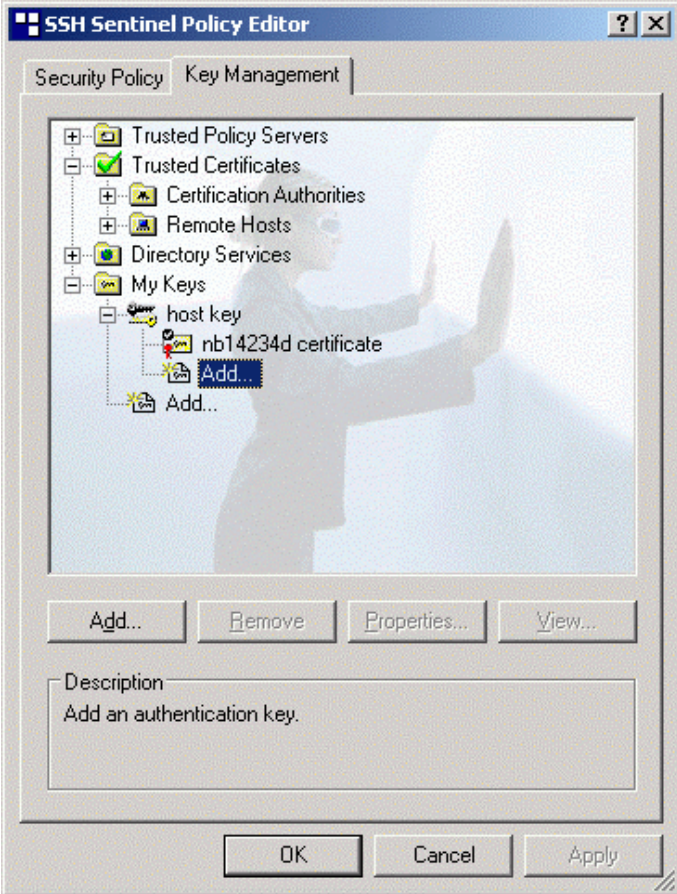
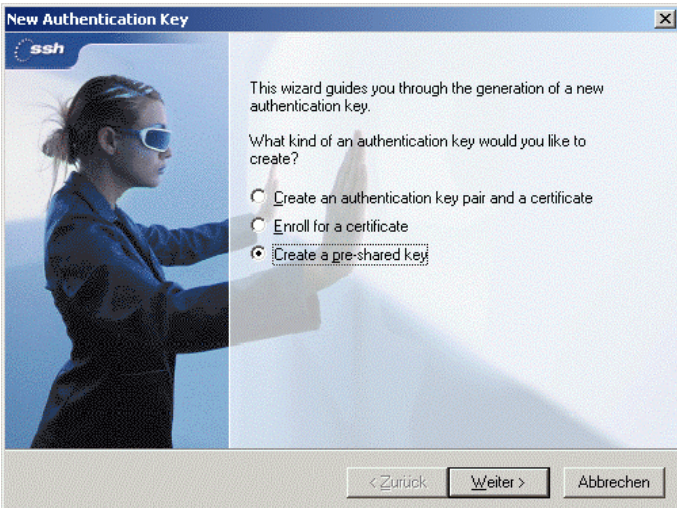
Table 2-4


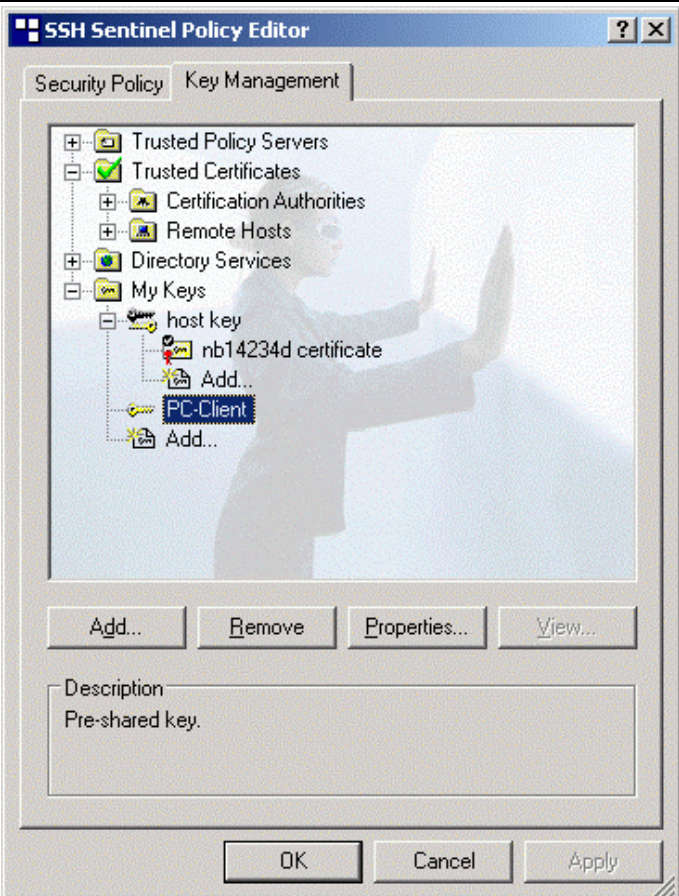
No.	Action	Note
1	Ensure that the mouse is kept in constant motion in this figure. Otherwise, the installation progress bar will stop running.	

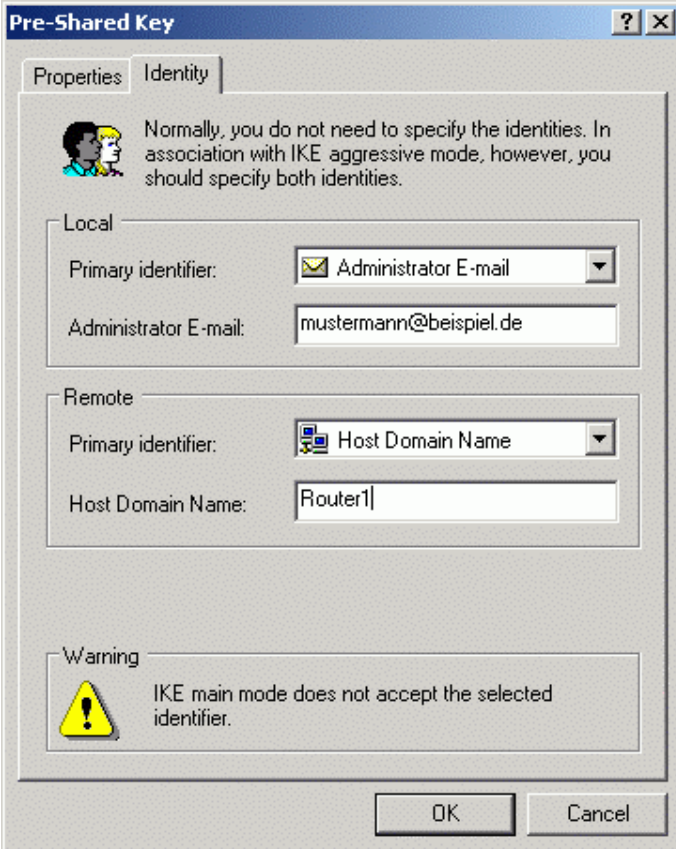
Copyright © Siemens AG 2004 All rights reserved
WinCC_flexible_Fernwartung_VPN_e.doc

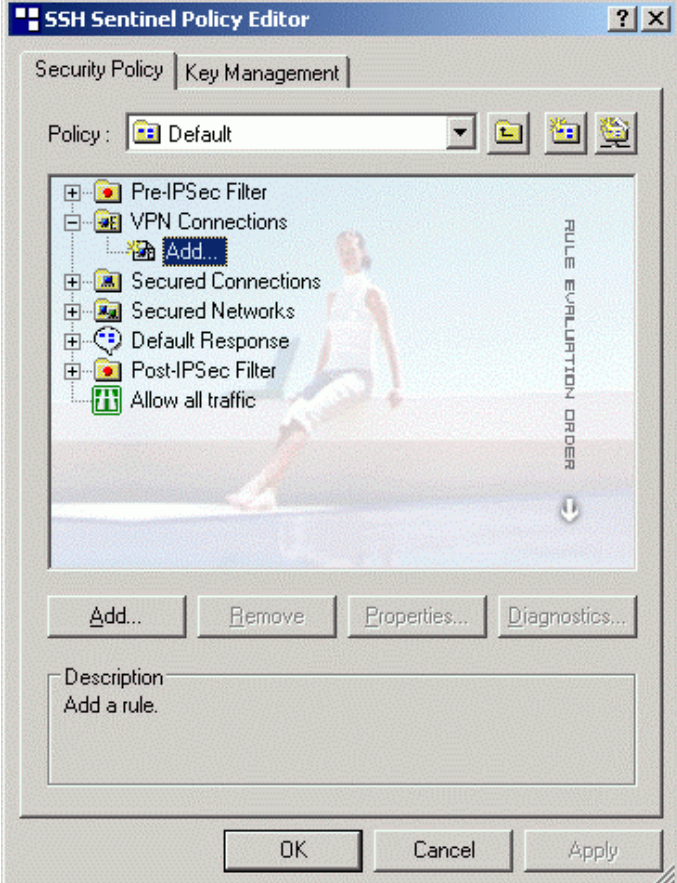

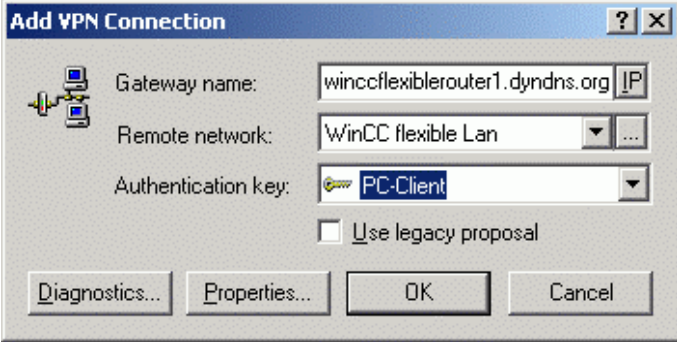
2	<p>Certain parts of the encryption are generated during this phase.</p>	
3	<p>Now specify your router's domain name.</p>	
4	<p>Select the first option in this window (Create a self-signed certificate) because you have not configured any certification on the router.</p>	

5	<p>The installation wizard performs diagnostics of the individual encryption algorithms. This completes the installation.</p>	
6	<p>After you restart your PC, the icon for the SSH Sentinel appears in your task bar. Right-click it to open the Policy Editor.</p>	

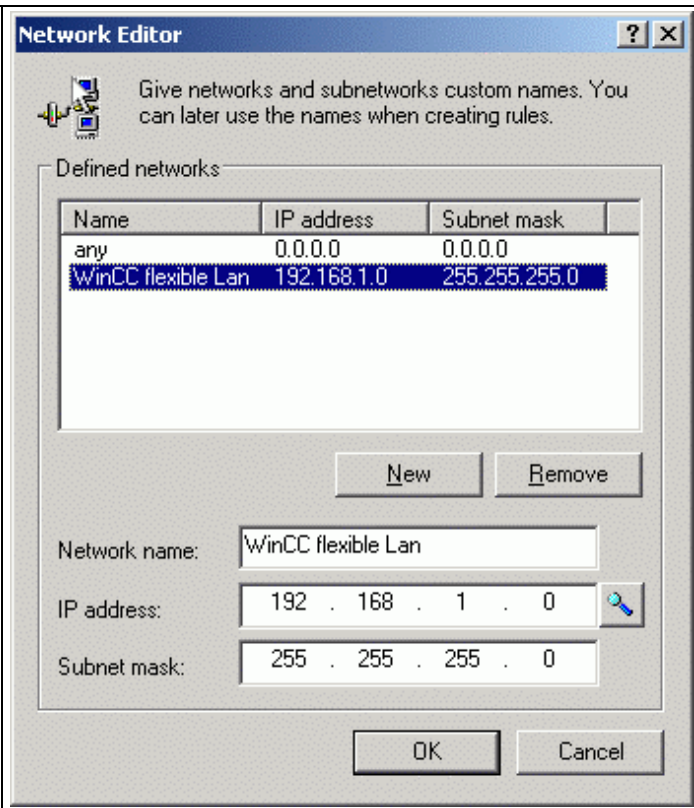
7	In the Key Management tab, click Add... to add a new key to the My Keys folder.	
8	Select the Create a pre-shared key option.	

9	<p>The name of the key is user-definable. Under Shared secret, enter the Pre Shared Key that was previously entered in the router.</p> <p>After you click Finish, you still need to define further settings in the key properties.</p>	
10	<p>To do this, select your newly created key and click Properties...</p>	

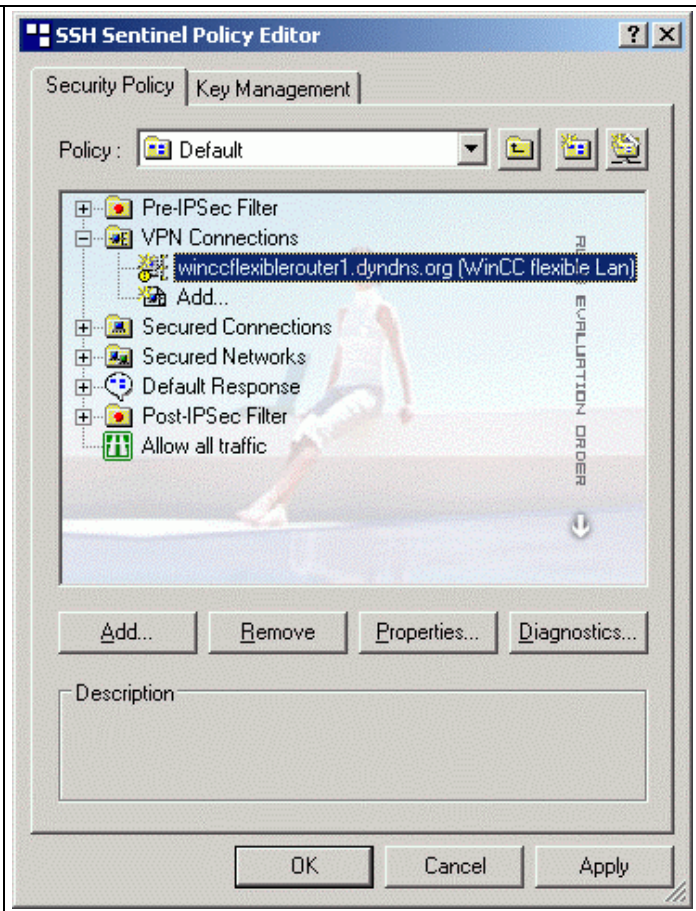
<p>11</p>	<p>The Local > Primary Identifier corresponds to the value of the peer IDs which have been configured in the router.</p> <p>The Remote > Primary Identifier must correspond to the router name entered for local ID.</p> <p>These settings conclude the configuration of the key.</p> <p>Note: These are the entries that you made a note of previously from the PC-client peer configuration for your router.</p>	 <p>Pre-Shared Key</p> <p>Properties Identity</p> <p>Normally, you do not need to specify the identities. In association with IKE aggressive mode, however, you should specify both identities.</p> <p>Local</p> <p>Primary identifier: Administrator E-mail</p> <p>Administrator E-mail: mustermann@beispiel.de</p> <p>Remote</p> <p>Primary identifier: Host Domain Name</p> <p>Host Domain Name: Router1</p> <p>Warning</p> <p>! IKE main mode does not accept the selected identifier.</p> <p>OK Cancel</p>
-----------	---	--

<p>12</p>	<p>You still need to create the actual VPN connection for contacting the router.</p> <p>In order to do this, go to the VPN Connection folder in the Security Policy tab and click Add... to add a new connection.</p> <p>Multiple keys as well as multiple connections can be configured in the Policy Editor.</p> <p>However, only one connection can be started.</p>	
<p>13</p>	<p>First of all enter the DynDNS name or IP address of your router as the Gateway name. However, using the IP address only makes sense if your router has a permanent address on the Internet.</p> <p>As regards the Remote Network, you can use the default "any" or click the  button to create a remote network yourself with your router's local network parameters.</p> <p>As far as the Authentication Key is concerned, use the key that is also saved on the router.</p>	

- 14 The values from this example are shown here.
Only again, you only need to specify the starting address. Specifying the remote network has no bearing on the encryption.
Click **OK** to confirm all the dialogs.



- 15 Adjustments now need to be made in the connection properties which concern authentication via the aforementioned algorithms. In order to do this, open the next dialog by clicking the **Properties...** button again.



- 16 In the **General** tab, click the **Settings...** button under the **IPSec / IKE proposal** option.

Note:

The source IP address for the data packages can be adapted in the settings under **Acquire Virtual IP address**.

A virtual IP can either be entered manually or be obtained by DHCP.

The router settings must be coordinated with it.

If the "Acquire Virtual IP address" option is not used, the ISP-assigned IP address is used as the source IP address.

The "Acquire Virtual IP address" option has not been used in this example.

Rule Properties

General Advanced

Remote endpoint

Security gateway: inccflexiblerouter1.dyndns.org IP

Remote network: WinCC flexible Lan ...

IPSec / IKE proposal

Authentication key: PC-Client

Proposal template: normal

Settings...

☐ Acquire virtual IP address

A virtual IP address is an address from the internal network. Settings...

☐ Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication. Settings...

Description

Change...

OK Cancel

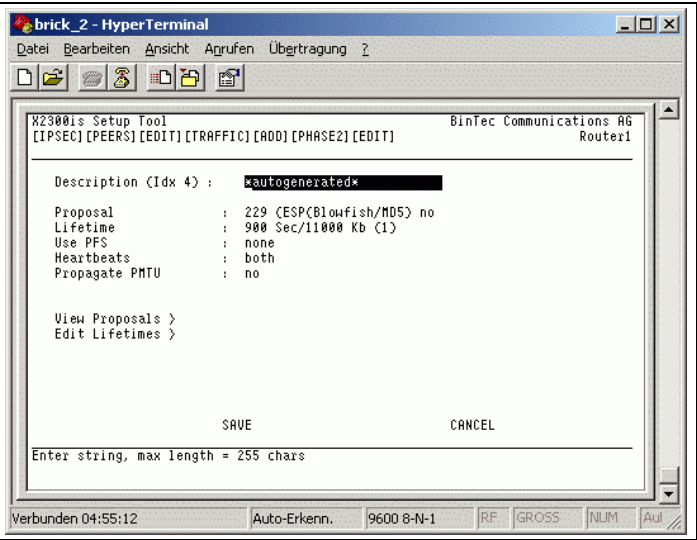
17 Note:
Since your computer is always assigned an official IP address by the provider on a dynamic basis, the **IKE Mode** provider must be set to **Aggressive Mode**.

This setting must also be selected accordingly on the router.

The settings for **Encryption algorithm** should be adapted to those on the router, as shown in Figs. 18 and 19.

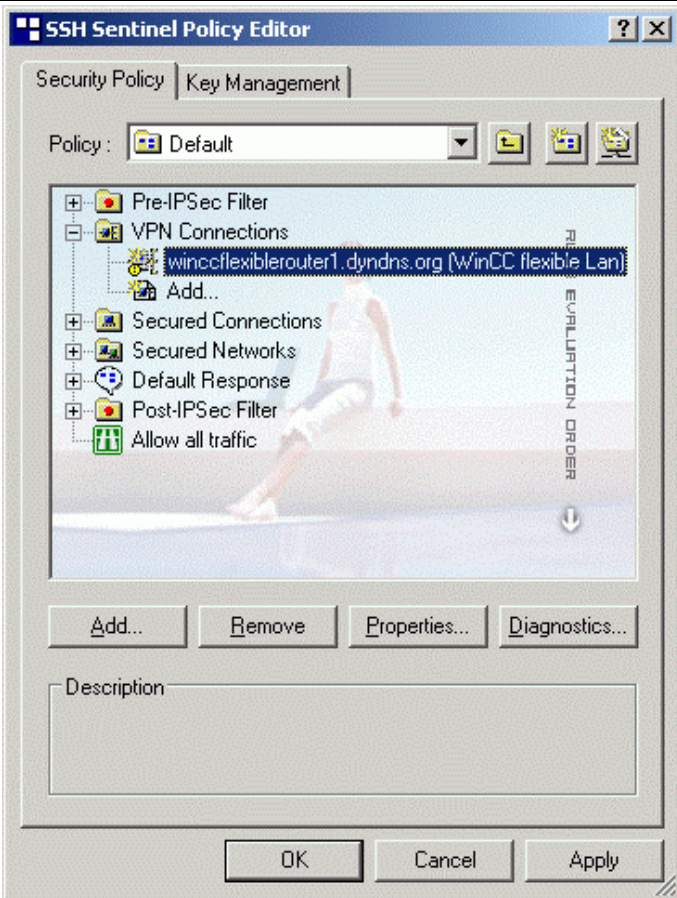
The client provides you with the full array of supporting encryption methods that can also be used in the router. Following completion of the data, click **OK** to close the dialog.

18 Comparison with the settings in the router for phase 1 of authentication. (IKE proposal)

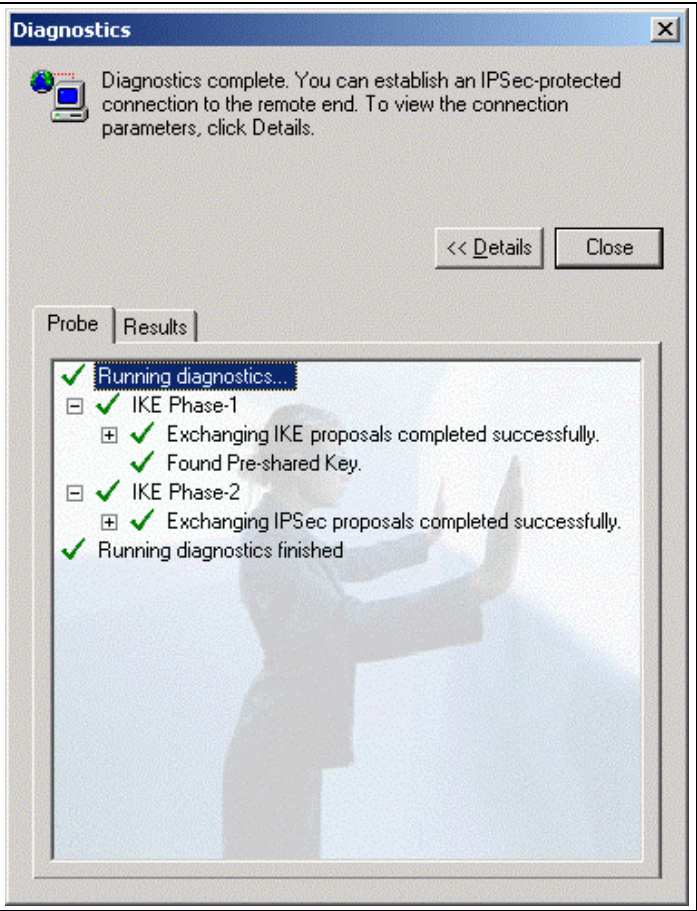
19	Comparison with the settings in the router for phase 2 of authentication. (IPSec proposal)	 The screenshot shows a HyperTerminal window titled 'brick_2 - HyperTerminal'. Inside, the 'X2300is Setup Tool' is running, specifically the '[IPSEC] [PEERS] [EDIT] [TRAFFIC] [ADD] [PHASE2] [EDIT]' screen. The settings for 'Description (Idx 4)' are as follows: - Proposal: 229 (ESP(Blowfish/MD5) no) - Lifetime: 900 Sec/11000 Kb (1) - Use PFS: none - Heartbeats: both - Propagate PMTU: no At the bottom, there are 'SAVE' and 'CANCEL' buttons, and a text entry field with the prompt 'Enter string, max length = 255 chars'. The status bar at the bottom of the window shows 'Verbunden 04:55:12', 'Auto-Erkenn.', '9600 8-N-1', and other interface elements.
----	---	--

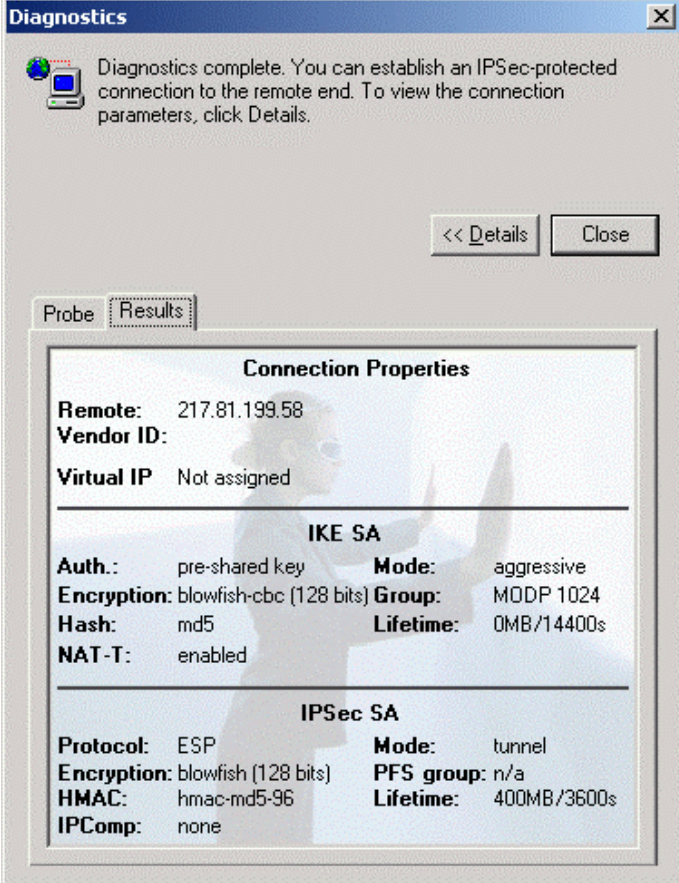
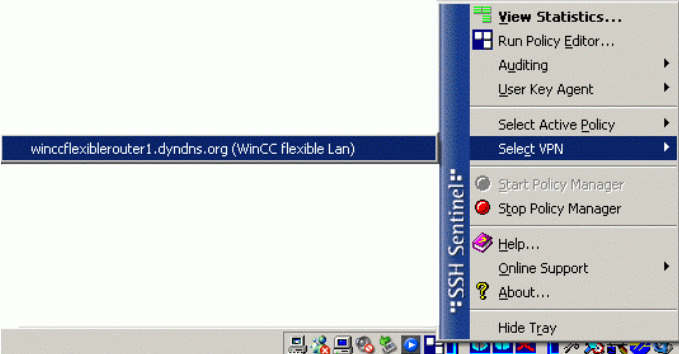
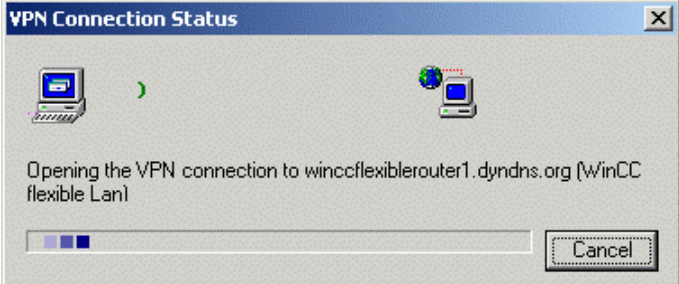
2.5 Testing the newly created connection:

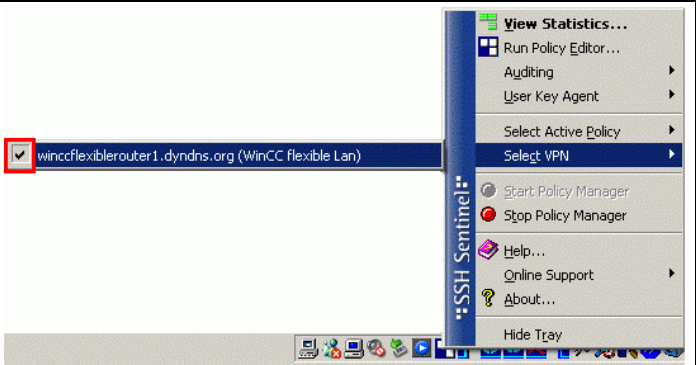
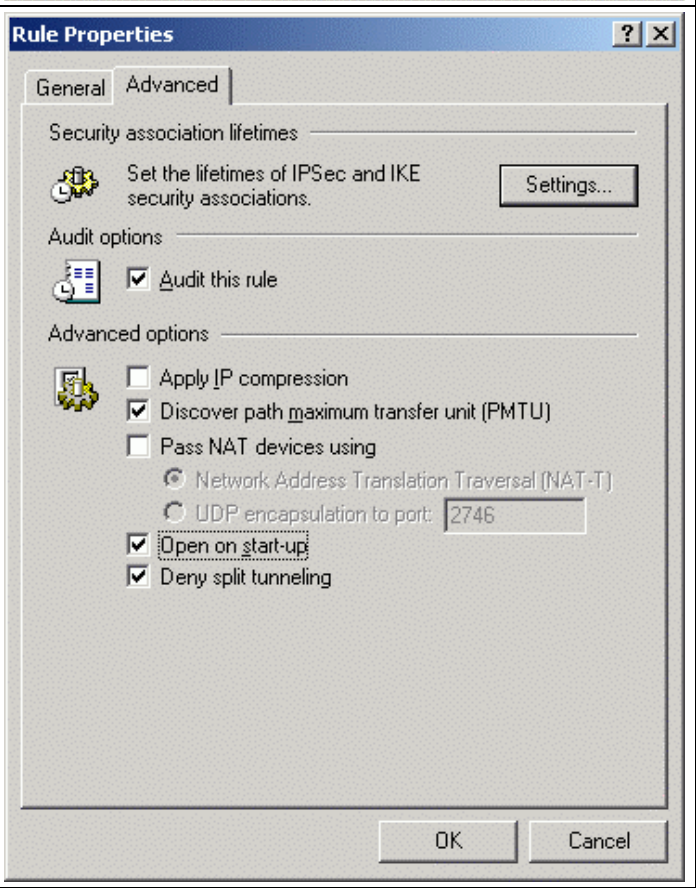
Table 2-5

No.	Action	Note
1	Start the remote connection to your Internet Service Provider. Open your Policy Editor again and select the requisite VPN connection. Click the Diagnostics... button to see whether encryption has been correctly detected.	

2 If everything is correctly set, the following dialog should appear.



3	<p>The Results tab shows how the connection is set. If it is incorrectly configured, only parts that have been correctly detected are ticked.</p>	
4	<p>Now close all the dialogs and right-click the SSH Sentinel icon in your taskbar. You can now view all the connections via the Select VPN option and activate them by selecting them..</p>	
5	<p>The connection is established.</p>	

6	Once the connection has been successfully established, the connection name is ticked.	
7	The tunnel can be established either manually by selecting Select VPN or automatically after connecting to the ISP. In order to avail of this option, the Open on start-up option must be enabled in the properties for your VPN Connection under the Advanced tab.	

This concludes the settings for your IPSec connections.

You can test them quickly and easily by pinging to an IP address in your company network.

If you fail to establish a connection, check all the settings in the router once again and compare them with your client.

For more precise troubleshooting, you can also contact your router manufacturer's Support hotline.

They use a debugger on the router directly to see which setting is incorrect. The debugger cannot be explained here.

3 Glossary

Table 3-1

No.	Abbreviation	Description
1	ADSL	<p>Stands for Asymmetric Digital Subscriber Line.</p> <p>ADSL supports the use of the infrastructure in the existing phone network for broadband utilities. Additional data for Internet utilities is transmitted on the copper two-core conductors of the analog and digital telephone lines (POTS or ISDN) in the case of ADSL. For this purpose, the spectrum of frequency used by ADSL is divided into several sections. This enables the telephony and data signals to be transported side-by-side between the subscriber's line and the local exchange. There is a splitter on either side to separate and combine the signals.</p> <p>In ADSL, the maximum transmission rate that can be achieved is asymmetric in both directions, upstream and downstream. ADSL supports upstream transmission of up to 1.5 MBit/s and downstream of up to 8 MBit/s. However, as the transmission rate which can be achieved drops significantly the further apart the local exchange and subscriber are, these values cannot be achieved in practice for the majority of lines.</p> <p>The asymmetric DSL variants, in which there is a speed of up to 256 kBit/s available for upstream and up to 3 MBit/s available for downstream, are particularly suitable for private users and small businesses who do not wish to make large volumes of frequently requested Internet content available on their PC for other users.</p>
2	BBAE	<p>Stands for Broadband Access Equipment.</p> <p>The BBAE represents a subscriber's terminal connection to a line that is used for broadband. It separates the provider network from the subscriber line cable and conditions the signals for transmission via the connection element.</p> <p>In the case of ADSL connections, the BBAE generally also features the splitter that separates the broadband and narrow band signals from one another and combines them again.</p>
3	CAPI	<p>Stands for Common Application Programming Interface.</p> <p>A standardized software interface for communication between software and hardware.</p> <p>CAPI is the name of a program which is supplied with an ISDN card and which is used to activate it. Other programs that wish to transmit data via the card only have to pass this data on to the CAPI driver.</p>
4	DSL	<p>Stands for Digital Subscriber Line.</p> <p>DSL technology enables data transmission to be accelerated substantially via conventional phone lines, making it especially suitable for high-speed Internet use. ISDN services or analog telephony continue to run undisturbed on the same line. The high transmission rates are achieved by enlarging the frequency range</p>

		<p>used. For example, ADSL supports transmission rates of up to 8 MBit/s. Lines with capacities of 768 kBit/s are very common.</p> <p>The name DSL represents a whole family of technologies that are combined under the collective term xDSL. In Germany, lines for private customers are mainly offered with asymmetric DSL (ADSL) and single pair DSL (SDSL) technologies. ADSL, which is much more common, transmits the Internet data in the existing telephone network above telephony frequencies between 138 and 1,104 kHz. For example, ADSL is also the basis for the T-DSL product offered by Deutsche Telekom AG.</p>
5	DynDNS	<p>The term DynDNS stands for dynamic DNS and is meant to indicate that you as the customer can enter the IP address belonging to a name in the DNS server yourself.</p> <p>The partner's IP address is contacted, and the connection is established. However, since fixed IP addresses are expensive, most users connect to service providers and are assigned a dynamic IP address.</p> <p>This changes every time you connect (hence the term dynamic), making it impossible to locate a partner with a dynamic IP address. DynDNS servers on the Internet offer assistance in this respect. They enable partners to be located despite their dynamic IP address. If the partner is known, i.e. if its IP address is known, there is nothing to prevent communication. In the interests of security, communication with the partner can be encrypted with the aid of IPSec, for example, in a second step.</p>
6	IPsec (Internet Protocol Security)	<p>IPSec is a protocol that can be used to establish a secure IP connection.</p> <p>A distinction is made between two modes:</p> <ol style="list-style-type: none"> 1. Tunnel mode The entire IP package is encrypted in this mode. Tunnel mode is primarily used to transmit data between two company locations or between a private PC and a company network (to enable staff to work from home, for example) via the Internet secure from monitoring (VPN). 2. Transport mode Here only the data part is encrypted. This is used to transmit critical data, e.g. in passwords.
7	ISDN	<p>Stands for Integrated Services Digital Network.</p> <p>The striking feature of ISDN phone lines is that there are at least two basic access channels (B-channels) available for use simultaneously. This means that a subscriber is contactable by phone whenever it is online or sending a fax. It also supports two parallel phone calls from one line. In addition, higher transmission rates are possible than with an analog line. Each B-channel can transmit 64 kBit/s, i.e. the two together support 128 kBit/s.</p> <p>ISDN digital transmission and switching technology supports diverse forms of communication on the phone line such as telephony, faxing or Internet connections.</p> <p>ISDN continues to use the cabling from the previous analog telephone</p>

		network in order to connect the customers to the exchange. However, ISDN technology uses this with much greater efficiency and flexibility. Connections can be established more quickly, speech quality is much improved, and not only is data transmission is quicker, it is also extremely reliable thanks to error correction.
8	NTBA	<p>Stands for Network Termination Basic Rate Access.</p> <p>The NTBA forms the network termination to the public ISDN network. It converts the signal from the network provider from its two-wire line (UK0 bus) to a four-wire line (S0 bus).</p> <p>The exchange supplies current to the NTBA via the ISDN supply voltage – the NTBA, in turn, supplies the S0 bus. In normal operating mode, power is also fed to the NTBA via a power supply unit. In this mode it can supply up to four terminals which are connected to the S0 bus and which do not possess a power supply of their own.</p> <p>If the NTBA is operated without an additional power supply unit or if the power supply fails, the NTBA uses the network provider's ISDN supply voltage in order to operate on standby.</p>
9	Port Forwarding	<p>Port forwarding is a technology which supports the mapping of ports to IP addresses in NAT networks (Network Address Translation), i.e. if router ports have to be forwarded permanently to a specific IP address. This mapping technology is a function offered by many of the current DSL routers. For this purpose, the advanced settings for the router generally include a table in which a port that has to be mapped is permanently allocated to a specific local IP address.</p>
10	Router	<p>Routers are first and foremost hardware devices or software programs that can be used to connect one or more computers or whole networks to other networks.</p> <p>The router acts as the control center in order to forward connection requests to the required network or the service.</p> <p>In addition to their basic functionality, hardware routers and, in particular, the current ISDN or DSL routers possess DHCP services or servers which can be used to manage address allocation and control centrally. Depending on the settings, IP addresses can be supplied in this way to whole networks, which is beneficial to inexperienced users, in particular.</p>
11	Splitter	<p>Splitters</p> <p>In ADSL lines, the splitter divides the incoming signal from the provider network into the broadband ADSL signal and the narrow band ISDN signal or analog telephone signal. For transmission in the opposite direction, the two parts of the signal are combined to facilitate simultaneous transmission via the subscriber line.</p> <p>The splitter is frequently contained directly in the broadband access equipment (BBAE).</p>
12	TCP	<p>TCP, which stands for Transmission Control Protocol, is an important component of the TCP/IP protocol. It is based on connections and requests receipt of confirmation for every package sent.</p>

13	TCP/IP	TCP/IP stands for Transmission Control Protocol/Internet Protocol. This generally refers to the whole family of protocols. It was developed to facilitate connection between computers in different networks. Nowadays TCP/IP is used in many LANs (Local Area Networks) and is the basis for the world wide web.
14	T-DSL	Deutsche Telekom has been offering DSL lines under the name T-DSL since the late 90s. T-DSL is the most commonly used variant of DSL, which also makes it the most common type of broadband Internet access in Germany. Deutsche Telekom is not the only organization which offers T-DSL access to the Internet via its subsidiary T-Online, this is also available from a relatively large number of resellers. However, they all use Deutsche Telekom infrastructure to establish the physical link to the customer. The remaining providers primarily use their own versions of ADSL or else SDSL, although this works symmetrically and supports data rates of up to 2.3 MBit/s.
15	VPN (Virtual Privat Network)	Company employees can use a Virtual Private Network (VPN) to connect to the company network (Intranet) from home or from locations outside the company via the Internet. A number of company sites can also be linked this way. The advantage of this is that there is no need for modem links or leased channels, simply a connection to the Internet. The employee connects to the Internet first of all. An encrypted channel (tunnel) is then established between the VPN client and VPN server. Following authentication via user name and password or public key/certificate, an encrypted IPSec tunnel is set up via which data can be transmitted without risk of being monitored.
16	WAN	The term WAN (Wide Area Network) refers to networks which transmit data over a larger distance than a LAN (Local Area Network).

4 **Warranty and Support**

No liability is accepted for the foregoing or following internal Siemens information.

A&D accepts no liability, regardless of the legal grounds, for damages arising from the use of the examples, tips, programs, configuration and performance data, etc. described in Expert Communications, apart from the statutory liability accepted, for example, for damage to items used for personal purposes, personal accidents or for malicious intent or gross negligence.