VIRTUAL PRIVATE NETWORKING

September 2002

VIRTUAL PRIVATE NETWORKING

Table of Contents

REFERENCE

1 Technology Overview

1.1 Introduction

A Virtual Private Network can be considered as a virtual Wide Area Network. It is "Virtual" in the sense that the network is not physical but is established on demand by software that establishes a link between two communicating sides. VPNs are typically established over public (TCP/IP-based) data networks such as the Internet.

Internet VPNs In Internet VPNs, companies set up connections to their Internet Service Providers (ISP) and let the ISP transmit the data to the desired destination across the Internet. Virtual also implies that the networks are dynamic. Connections are established on demand and torn down when they are no longer needed, reducing bandwidth utilization and consequently costs, especially for dial-in clients. LAN-to-LAN VPN connections (typically with a leased line connection to the ISP on one side, a dial-up line on the other) also offer significant cost savings in comparison with long-distance dedicated lines.

Security As the Internet is a public network with the security risks associated with the open transmission of data, companies that rely on Internet VPNs depend on the encryption of their data to prevent the threat of security violations, such as spoofing, sniffing or man-in-the-middle attacks. A VPN is thus considered a Virtual "Private" Network since user data transmitted over the link is typically encrypted. Windows 95/98/NT/2000 based networks achieve this security via Microsoft's own Point-to-Point Encryption protocol, or MPPE. This encryption method was developed especially for use with the protocol PPTP, a major tunneling protocol.

Tunneling protocols There are three major tunneling protocols: IPSec, L2TP and PPTP.

- IPSec is an advanced security package that addresses issues such as authentication, key management, data privacy and integrity, as well as supporting VPN tunneling. Due to the inclusion of such security measures in its standards set, it provides an excellent security solution for pure IP environments. IPSec operates at layer three and can thus only transmit IP packets over its tunnels.

- The Layer 2 Tunneling Protocol (L2TP) is a hybrid Layer two tunneling protocol that combines elements from PPTP and L2F (a proprietary product from an American manufacturer). Like PPTP, L2TP leans heavily on PPP; the ability to use IPSec increases the security of data transmission.
- The Point-to-Point Tunneling Protocol or PPTP is an IETF standard described in RFC 1171. PPTP works at layer two, the Link layer enabling PPTP to work in multiprotocol environments such as IPX and NetBEUI as well as IP. PPTP is especially popular in Client-LAN VPNs as the protocol is supported by Windows operating systems.

The VPN solution that is described in this document and that can be acquired as an extended feature from BinTec Communications AG is the PPTP VPN.

1.2 Tunneling and PPTP

The process of building a VPN tunnel between a PPTP client and a VPN partner can be outlined as follows.

How a tunnel is built

Initially, a fully authenticated, standard, physical PPP link is made to an ISP. Once the PPP link has been established, a second logical connection, this time using the PPTP protocol, is made to the VPN partner over the physical interface to the ISP. Therefore, PPTP uses the PPP link to the ISP as a vehicle to estab-

lish a tunnel over the infrastructure of the Internet to its VPN partner and to exchange user data packets with this other tunnel endpoint.

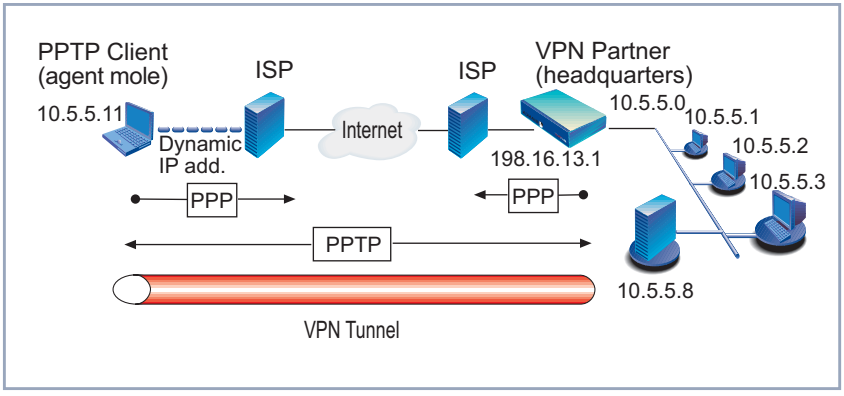

Figure A-1: Typical VPN scenario

Control connection

In order to do this, PPTP creates a control connection that contains control packets and that runs over TCP. The control packets forward messages that establish, maintain and end the connection between the two PPTP tunnel endpoints.

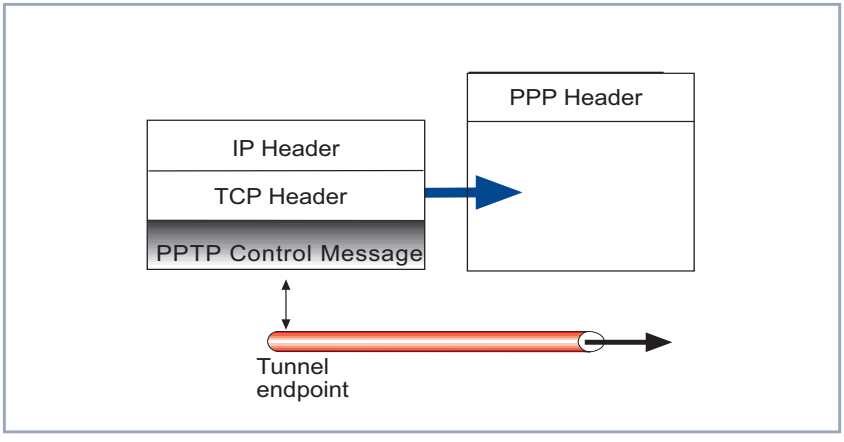

Figure A-2: Tunnel establishment phase

Data stream

After the control connection is made, the PPTP protocol creates a data stream that contains data packets that run in IP envelopes, using GRE (GRE refers to the Generic Routing Encapsulation protocol). After the PPTP tunnel is estab-

lished, the actual user data transmission can commence over this data stream, see figure A-7, page 15.

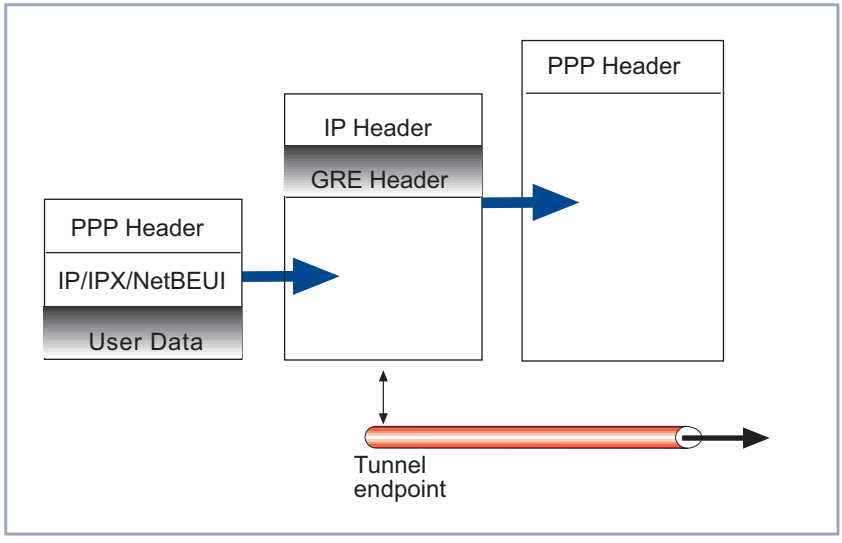

Figure A-3: Data transport phase

When sending data, PPP packets are encapsualted in the user-data field of the IP packet which is later unpacked by the opposite site.

1.3 Network Address Translation

For both basic Internet access as well as for the construction of a VPN over the Internet, the use of Network Address Translation (NAT) offers significant advantages.

- A limited number of official IP addresses is required for the entire LAN. This saves costs for the organization and conserves the number of world-wide exclusive IP addresses.
- Security is increased by hiding internal IP addresses from external networks, while at the same time enabling all workstations to access the Internet and participate in VPN tunnels.

- The reconfiguration of workstations in the LAN is not necessary.

1.3.1 The Conversion of Addresses

Address translation without VPN

The Network Address Translation feature on the BinTec router converts internal IP addresses in IP packets destined for the public Internet, substituting a globally unique address for the private address within the packet. The globally unique address, automatically converted in the **ipNatTable**, becomes the source address of the IP packet. When the globally unique address returns to the BinTec router, it is reconverted to the originating LAN IP address by means of the port number accompanying the packet.

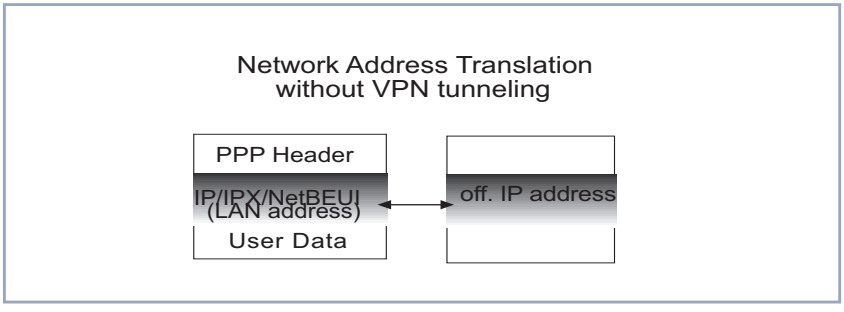

Figure A-4: Address translation without VPN

Address translation with VPN

Network Address Translation occurs a little differently when the BinTec router is functioning as a VPN tunnel endpoint. In this case, the LAN IP address is not converted to a globally unique IP address as outlined above. What happens is this: the packet the VPN router receives from the LAN, including the LAN IP address is packed within the IP packet of the VPN tunnel endpoint. The LAN IP address is thus "absorbed" within another IP packet. This absorbing IP packet, the IP packeting of the VPN tunnel endpoint, uses its own source address in the IP header, i.e the source address of the router. This source address may be the Unique Source Address, the LAN IP address of the router or the official IP ad-

dress. The source address, whatever it may be, is then translated through NAT into a globally unique IP address.

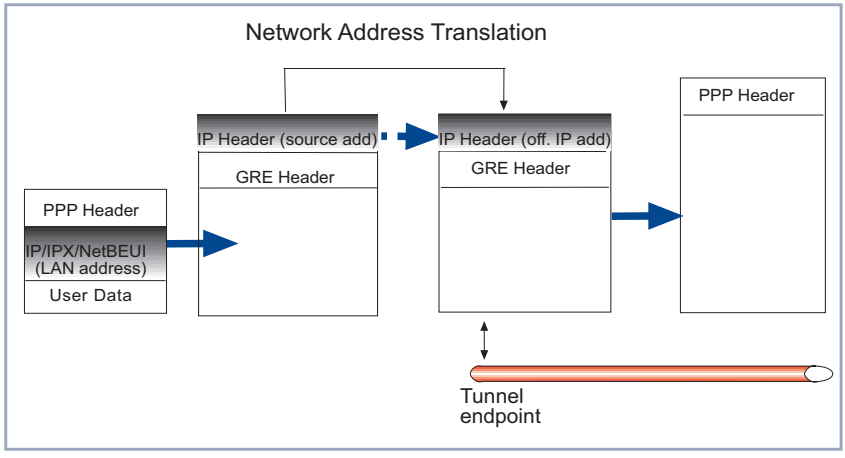

Figure A-5: Outgoing address translation with VPN

It could well be the case that the source address of the IP router is the same as the globally unique address and thus a translation of the former to the latter will not produce any visible difference. Nevertheless, strictly speaking a conversion from the router´s source address to the official IP address has taken place. The two addresses may differ, however, if the source address of the router is a Unique Source Address or the LAN IP address.

In non-VPN address translation, the source address of an outgoing session and the destination address of an incoming session are both the same for the same machine: the internal LAN IP address.

In VPN address translation, the source and destination addresses are different as the router itself is the source and destination and usually has different addresses for each. The router´s source address could be the official IP address, a unique source address or a LAN IP address, while the router´s destination address is invariably the loopback address (127.0.0.1) – which is basically a signal to unpack the tunneling headers and to send the remains back inside the LAN.

If NAT does not seem apparent when the router´s source address is the same as the globally unique address, i.e. the actual address does not change, the conversion of addresses is clearly perceptible when packets return to the VPN

tunnel endpoint. In this case, the official IP address is translated into the destination address (usually the loopback address). The tunnel packeting is then stripped away, leaving the user data and LAN IP address which is routed back into the LAN to the host requiring the data.

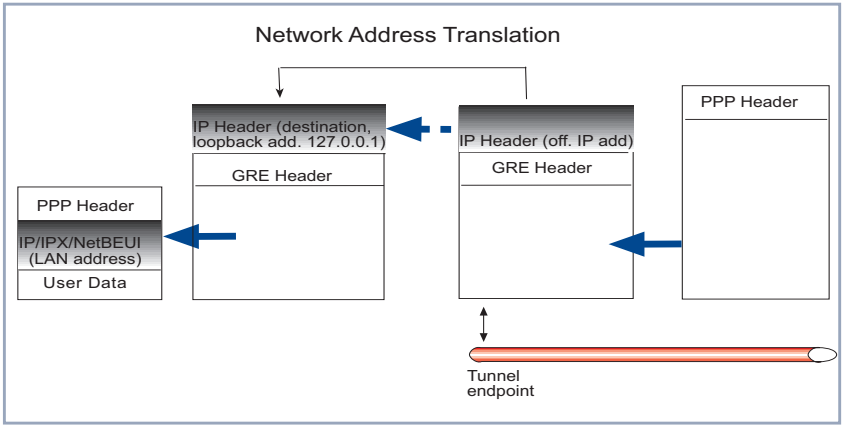

Figure A-6: Incoming address translation with VPN

1.3.2 VPN and NAT (session profiles)

With NAT activated on the ISP interface, the successful construction and operation of a VPN tunnel would ordinarily be prevented. GRE packets initiated by the VPN partner would not be switched through the NAT barrier. In order to ensure that packets can return to the LAN client that establishes the VPN connection and that lies concealed behind the BinTec router because of NAT, explicit permission for special session profiles must be given.

BinTec's NAT implementation supports connections with the protocols ICMP, TCP, UDP and GRE (Generic Routing Encapsulation).

The administrator can specify these session profiles by means of the following parameters:

- The type of service used; or a combination of the port number used (e.g. 1723) and the protocol used (e.g. TCP).

- The particular IP address that may be allowed through the NAT barrier.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

To allow FTP sessions, for example, the tcp protocol and port 21 would have to be configured (**IP ➧ NAT ➧ Config ➧ ADD**).

TCP and GRE

For the specific purpose of establishing a VPN connection with PPTP over NAT, the protocols TCP and GRE must be allowed through the NAT barrier.

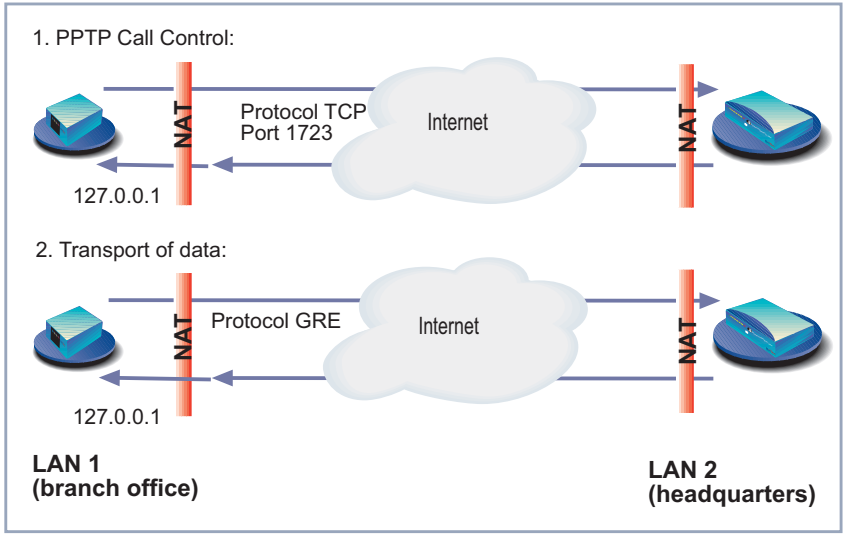

Figure A-7: TCP and GRE switched through a NAT interface

In the example above, NAT is activated on the ISP interface of ***branch office***. The VPN connection can only be realized by ***headquarters*** if both the TCP and GRE packets from ***headquarters*** can be switched through the NAT firewall of ***branch office***. The reverse is also the case in the example. TCP and GRE packets must be allowed through the NAT firewall of ***headquarters*** so that ***branch office*** can establish and transmit data to ***headquarters***. As explained above, once both protocols, TCP and GRE, have been given explicit permission to pass through the NAT firewall, the PPTP VPN tunnel can successfully exchange data over a NAT interface.

Firstly, TCP is switched through for the establishment of a tunnel.

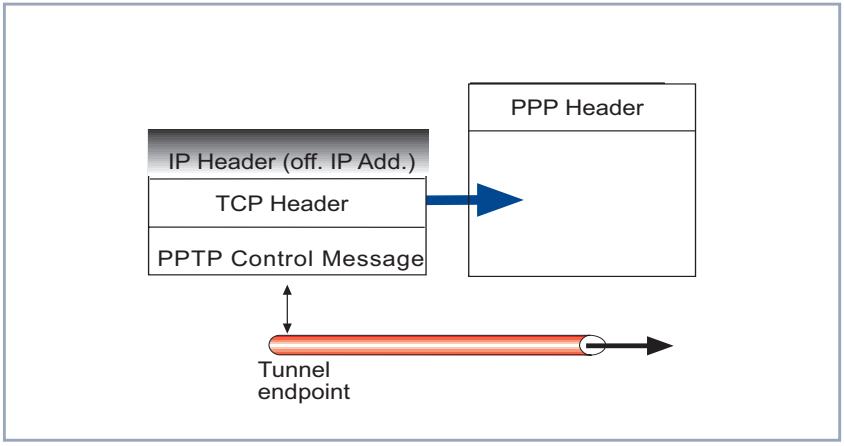

Figure A-8: Tunnel establishment phase

And then GRE is switched through to allow the data channel to be opened.

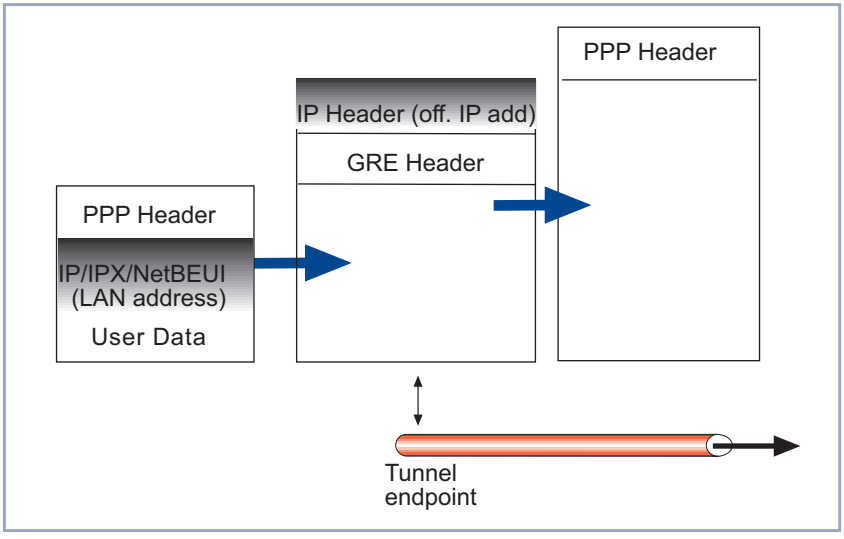

Figure A-9: Data transport phase

1.4 Authentication – Encryption – Compression

In the scenarios below (see section A, chapter 1.6, page 19), a second PPTP connection is established over an existing link. This second connection has its own PPP parameters (unique from those of the underlying ISP link) with respect to user authentication, encryption, and compression.

1.4.1 Authentication

Both the ISP and the VPN Server will typically want to verify the initiating partner during connection establishment. Authentication is performed inband using PAP, CHAP, or MS-CHAP. The authentication parameters for both the ISP and the VPN server connections are completely independent of each other.

1.4.2 Data Encryption

Data encryption allows you to be sure that all user data transmitted over public data networks via a VPN is secure. The BinTec router supports Microsoft's Point-to-Point Encryption protocol, or MPPE. Data encryption/decryption is performed at each end of the tunnel.

In addition, BinTec routers support the encryption protocols DES, Blowfish and Triple Blowfish. These protocols can thus be used in a LAN-LAN VPN.

Each host separately generates a session-key (40, 56 or 128-bit key) using the respective partner's PPP password which is known to each host. The passwords must be exchanged between partners and configured before an attempt to establish a VPN link can be made.

Since session-key generation is based upon the partner's password, data encryption is only possible if authentication (PAP, CHAP, or MS-CHAP) is enabled. Also, for 128-bit encryption the MS-CHAP authentication protocol is required (i.e. must be successfully negotiated at connect time).

The Windows PPTP configuration dialog includes an option for password encryption. This option applies to transmittal of the PPP password and does not apply to data encryption.

1.4.3 Compression

Depending on the data and the compression algorithm used, data compression can increase performance over dial-up links as much as 30 fold (best case scenario using Stacker LZS). In both scenarios shown below, compression can be enabled for the initial PPP connection. Compression can also be enabled for PPTP links between BinTec routers (see section A, chapter 1.6.1, page 19).

The following limitation currently exists when combining compression and encryption for a PPTP link with Windows 95 based hosts.

When the **Enable software compression** option is enabled in the **Server Types** tab, Windows 95 PPTP Clients offer either **MPPC Compression** or **MPPE Encryption** when tunnel parameters are negotiated. Currently, compression is only possible for the PPTP link if encryption is set to *none* for the VPN partner interface on the BinTec router.

1.5 Static and Dynamic IP Addresses

There are two different scenarios in which the manner of IP addressing on either side of the WAN affects which side can establish or partake in a VPN tunnel:

- One side has a statically configured IP address, the other does not.
  If the client gets its IP address dynamically assigned by its ISP, the VPN connection can only be established by that client, not by the central site.

The central site has to have a statically configured IP address to enable the client to establish a VPN connection to the central site.

- Both sides have a statically configured IP address.
  Assuming both sides have static IP addresses (LAN-LAN connection), the VPN connection can be established by both sites.

If neither side has a statically configured IP address, a VPN tunnel can not be established. In such a case, it is impossible for either side to establish a connection with a partner whose IP address is unknown.

1.6 Scenarios for PPTP VPNs

Here we will look at some of the most commonly used scenarios for establishing VPN connections.

- The first is where two LANs, both equipped with BinTec routers, build a VPN tunnel between their LANs.
- The second is where a LAN-LAN VPN tunnel is established after one side triggers the other side to call back.
- The third is where a roaming client (Win NT, for example) dials in to an ISP and establishes a VPN connection with his headquarters over the Internet.

1.6.1 LAN-to-LAN VPN Tunnel

In this scenario, a Virtual Private Network that connects two enterprise LANs via the Internet is established via two VPN servers. Both sides have BinTec routers

and both sides have statically configured official IP addresses. Either side may therefore initiate the VPN connection.

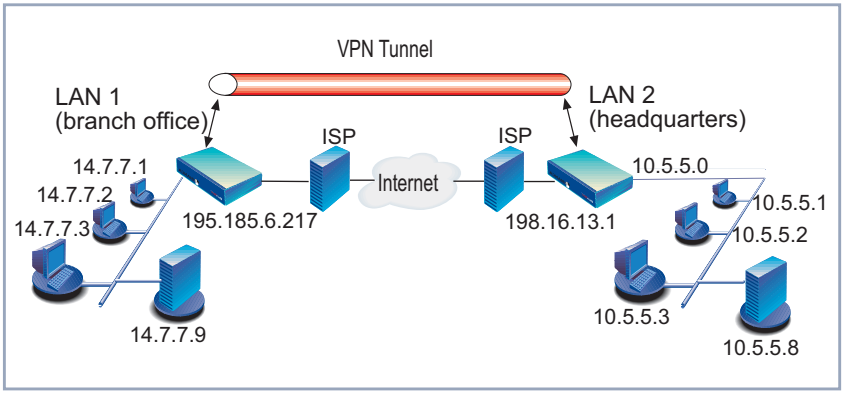

Figure A-10: LAN-to-LAN VPN (2 static IP addresses)

Firstly, a standard PPP link is made to a local ISP. Once the link is established, the same server, ***branch office***, establishes a PPTP connection to the remote VPN server ***headquarters***. Again, the ISP is unaware of its participation in the VPN.

All traffic routed via the ISP and destined for the remote LAN is encapsulated/unpacked by the respective VPN servers.

For the configuration of such a scenario, see section B, chapter 1, page 34.

1.6.2 LAN-to-LAN VPN Tunnel with Callback

Why Callback? Callback is not only useful to allow the side that cannot establish a VPN link (i.e. the side whose partner has no fixed IP address) to tell the side that can establish a VPN link to do so. In a scenario in which both sides are capable of estab-

lishing the VPN link (both sides have statically configured official IP addresses), Callback is very often required to simplify and regulate accounting systems.

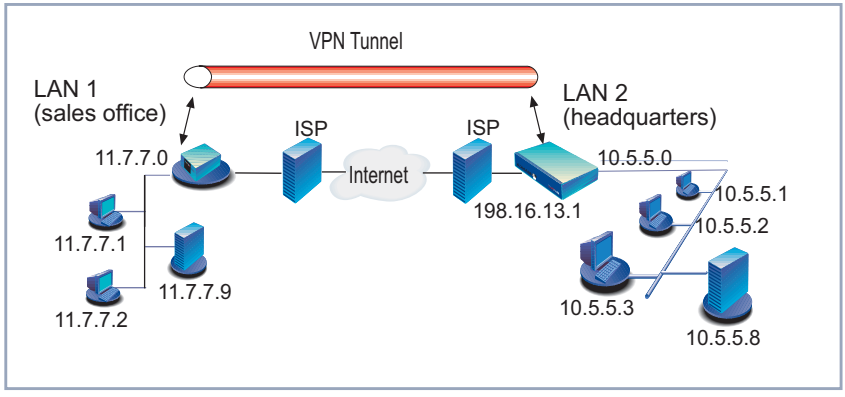

Figure A-11: LAN-to-LAN VPN (1 static IP address)

Triggering Callback

In this scenario, a Virtual Private Network that connects two enterprise LANs via the Internet is established via two VPN servers. Both sides have BinTec routers, but only ***headquarters*** has a statically configured official IP address. ***Sales office*** receives its IP address dynamically from its ISP. Therefore, only ***sales office*** can initiate the VPN connection. If, however, ***headquarters*** needs a VPN connection to be initiated (perhaps to transmit mails from the central server to the sales office), it can trigger the process with Callback.

For the configuration of such a scenario, see section B, chapter 2, page 42.

1.6.3 PPTP Client-to-LAN VPN Tunnel

This is one of two of the most common scenarios for PPTP. The remote client (***agent mole*** in the graphic below) first establishes a standard PPP connection to a local ISP. The same client then initiates a second logical connection to the VPN partner, ***headquarters***. The ISP (and all intermediate Internet routers),

unaware that it is participating in a VPN, simply routes IP packets from ***agent mole*** to ***headquarters***.

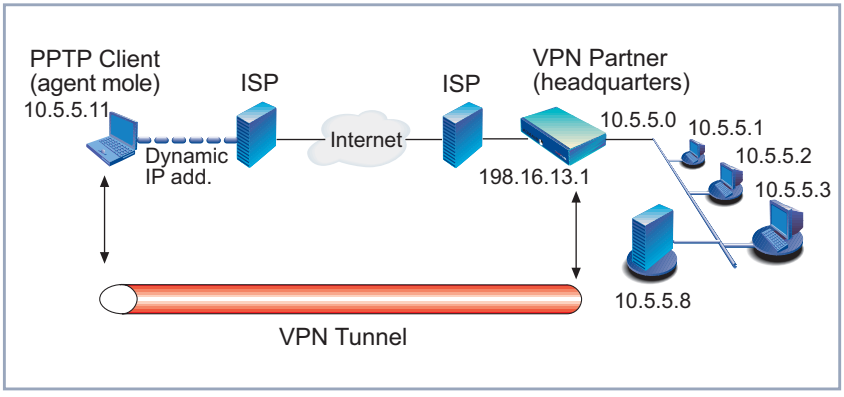

Figure A-12: Scenario 1: PPTP Client (teleworker) to VPN Server (LAN side)

To hosts on the Private Enterprise LAN, ***agent mole*** appears as if it were directly connected to ***headquarters***. The reverse also appears to be the case.

For the configuration of such a scenario, see section B, chapter 3, page 48.

2 Configuration Overview

2.1 Configuration over Setup Tool

After entering `setup` from the SNMP-shell prompt, Setup Tool's Main Menu is displayed as below. Depending on your hardware setup, software configuration and license agreements, your router's menu may differ slightly. The Setup Tool menu pages illustrated in this document are based on system software 5.2.1.

```
BinTec router Setup Tool                          BinTec Communications AG
                                                                  MyRouter


Licences                  System

Slot1:                    CM-BNC/TP, Ethernet
Slot2:                    CM-2XBRI, ISDN S0, Unit 0
                          CM-2XBRI, ISDN S0, Unit 1

Slot3:                    CM-1BRI, ISDN S0

WAN Partner
IP      IPX     X.25      VPN

Configuration Management
Monitoring and Debugging
Exit



Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

This overview will just take a look at the menu pages specific to VPN, the WAN partner entries necessary to configure a PPP link to an ISP can be found in a copy of the User´s Guide.

If you go to ***VPN***, you will find a list of the current Virtual Private Networking partner interfaces configured on the router.

```
BinTec Setup Tool                              BinTec Communications AG
[VPN]: Configure VPN Interfaces                                MyRouter


Current VPN Interfaces

        Interface            Protocol             State



            ADD              DELETE           EXIT
```

2.1.1 Creating VPN Interfaces

By pressing **ADD**, you will arrive at a menu where it is possible to create Virtual Private Networking interfaces:

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD]: Configure VPN Interfaces                           MyRouter

Partner Name                           H.Q.

Encapsulation                          PPP
Compression                            none
Encryption                             MPPE 128


PPP>
Advanced Settings>

IP >
IPX >


                     SAVE                CANCEL

Enter string, max length = 25 chars
```

The following is a list of fields and their meanings that need to be configured:

Field	Meaning
Partner Name	The partner name assigned to this virtual interface.
Encapsulation	The type of encapsulation to use; currently PPP must be used.
Encryption	Determines the type (if any) of encryption to use with this partner. Type of encryption depends on your system software. Microsoft Point-to-Point Encryption (MPPE) using 40-bit, 56-bit or 128-bit keys are supported. Additionally, BinTec routers support the encryption protocols DES, Blowfish and Triple Blowfish. These protocols can be used in LAN-LAN VPNs.

Table A-1: ***VPN*** ➧ **ADD** ➧ ***CONFIGURE VPN INTERFACE***

2.1.2 PPP Settings

In the ***PPP*** submenu, PPP settings for the VPN partner interface can be defined.

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD][PPP]: PPP Settings (H.Q.)                           MyRouter



Authentication                  MS-CHAP
Partner PPP ID                  HQ-ppp-id
Local PPP ID                    mybrick
PPP Password                    *******

Keepalives                      off
Link Quality Monitoring         off


                OK                          CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Authentication	The authentication protocol to use when authenticating this partner.
Partner PPP ID	The PPP ID that the VPN partner must identify itself with during PPP negotiation.
Local PPP ID	The BinTec router's PPP ID which is used during PPP negotiation with this VPN partner.
PPP Password	The password the VPN partners must use when challenged by the BinTec router during PPP negotiation. When entered in Setup Tool, each character is displayed as an asterisk. If Setup Tool is opened with the command `setup -p`, the characters of all passwords are not displayed as asterisks, but as legible entries.
Keepalives	This option is relevant for leased line connections and VPN connections. Keepalive packets are sent at regular intervals to test the status of the partner. It is advisable to set this feature to **on**.
Link Quality Monitoring	This option allows you to tell the BinTec router to gather PPP Link Quality statistics for a specific PPP partner. When enabled, link statistics are continously written to the BinTec router's **biboPPPLQMTable** (viewable from the SNMP shell), when a connection is established with this partner. It is usually unnecessary to enable this.

Table A-2: ***VPN*** ➧ **ADD** ➧ ***PPP***

2.1.3 Advanced Settings

In this menu, if using short hold, you should be careful to set the short hold for the VPN interface to a value shorter than the short hold value set for the interface to the ISP.

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD][ADVANCED]: Advanced Settings (H.Q.)                 MyRouter


Static Short Hold (sec)                    30
Extended Interface Settings (optional) >


                 OK                    CANCEL

Enter string, max length = 25 chars
```

The menu contains the following fields:

Field	Meaning
Static Short Hold (sec)	This is the time in seconds after the last exchange of data that the router waits before terminating the connection.
Extended Interface Settings (optional)	Advanced settings applying to the feature Bandwidth On Demand can be configured in this submenu.

Table A-3: ***VPN*** ➧ **ADD** ➧ ***ADVANCED***

2.1.4 IP Settings

The next Setup Tool menu we want to look at is the ***IP*** submenu. This is where IP addresses (official and/or unofficial) can be entered.

```
BinTec Setup Tool                                BinTec Communications AG
[VPN][ADD][IP]: IP Configuration (H.Q.)                          MyRouter


VPN Partner's IP Address              198.16.13.1
via IP Interface                      ISP
Identification by IP Address          yes

local IP Address

Partner's LAN IP Address              10.5.5.0
Partner's LAN Netmask                 255.255.255.0

Advanced Settings>

                 SAVE                 CANCEL

Enter string, max length = 25 chars
```

The menu contains the following fields:

Field	Meaning
VPN Partner's IP Address	The VPN partner's official IP address where the partner can be reached on the Internet.
via IP Interface	The IP interface that packets to and from this VPN partner will be sent and received on. This will typically be the interface to the Internet Service Provider.
Identification by IP Address	When set to *yes*, the VPN partner can be identified by his IP address (static).
local IP Address	For VPN interfaces, it is not recommended to make any entry here.
Partner's LAN IP Address	The VPN partner's LAN address.

Field	Meaning
Partner's LAN Netmask	The netmask the partner uses on its LAN. If left blank, a standard netmask for the respective network class will be used.

Table A-4: ***VPN*** ➧ **ADD** ➧ ***IP***

2.1.5 VPN Interface Settings

Now let´s take a look at the ***ADVANCED SETTINGS*** submenu.

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD][IP][ADVANCED]: Advanced Settings (H.Q.)             MyRouter


RIP Send                                      none
RIP Receive                                   none


Dynamic Name Server Negotiation               no


IP Accounting                                 off
Back Route Verify                             off
Route Announce                                up or dormant
Proxy Arp                                     off

                          OK                      CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
RIP Send/Receive	Defines which version of RIP packets to exchange with this partner.
Dynamic Name Server Negotiation	Defines whether (and how) the name server's address is configured. For a new DNS proxy feature see Release Notes 5.2.1.

Field	Meaning
IP Accounting	Enable/disable generation of IP accounting messages for this partner. When enabled, an accounting message is generated (and written in **biboAdmSyslogTable**) which contains detailed information regarding connection activity for this partner.
Back Route Verify	When enabled, the BinTec router verifies that the return route for all packets received from this partner interface uses the same interface the packet arrived on.
Route Announce	This option allows you to control when IP routes defined for this interface will be propagated. This is dependent upon the interface's **ifOperStatus** (in the **ifTable**) as follows: Possible values: ■ *up only*: Routes are propagated only when the operational status of the interface is up. ■ *up or dormant*: Routes are propagated only when the operational status of the interface is up or dormant. ■ *always*: Routes are propagated always, regardless of the current link's operational status.

Field	Meaning
Proxy Arp	Proxy ARP (Address Resolution Protocol) for WAN links is disabled, or *off* by default. When enabled (*up only* or *up or dormant*) requests are answered in dependence of the **ifOperStatus** of the link.

Table A-5: ***VPN*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

The settings defined here are similar to the ***WAN PARTNERS*** ➧ ***ADVANCED SETTINGS*** menu but apply specifically to a VPN partner interface.

2.1.6 IPX Settings

Finally, the ***VPN*** ➧ ***IPX*** submenu defines IPX-relevant settings for VPN partner interfaces that support IPX.

```
BinTec Setup Tool                                BinTec Communications AG
[VPN][ADD][IPX]: IPX Configuration (H.Q.)                        MyRouter


Enable IPX                yes
IPX NetNumber             0

Send RIP/SAP Updates      triggered + piggyback(on changes, per. if link
                          active)

Update Time               60


                  OK                          CANCEL

Enter hex number range 0..fffffffe
```

The menu contains the following fields:

Field	Meaning
IPX NetNumber	The IPX network number of the network link (the PPTP link). This is required by some IPX routers.

Field	Meaning
Send RIP/SAP Updates	Determines how often RIP and SAP packets are transmitted to this VPN partner. The possible options are the same as those defined in the menu, see the User's Guide for additional information.
Update Time	Determines how often (in seconds) periodic updates are sent to this VPN partner.

Table A-6: ***VPN*** ➧ **ADD** ➧ ***IPX***

WORKSHOP

1 How Do I Configure and Connect a LAN-to-LAN VPN

1.1 Introduction

Two distant networks, a corporate central site LAN ***headquarters*** and a partner's network ***sales office*** can be connected over the Internet via a Virtual Private Network using two BinTec routers as follows.

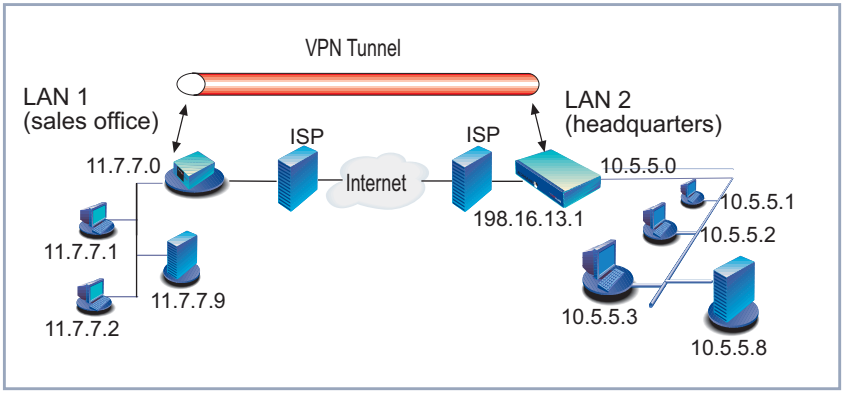

Figure B-1: Example LAN-to-LAN configuration

Once both BinTec routers are configured for Virtual Private Networking, hosts on either LAN can connect to hosts on the remote LAN. All traffic that is routed between the two networks is encrypted (user-data encryption).

The configuration

The configuration described below must be performed on both BinTec routers on each side of the WAN.

In essence, there are two stages involved in the configuration of each side of the VPN.

- Firstly, the configuration of the connection to the ISP over the PPP protocol. This is a perfectly conventional PPP connection and can be used for normal Internet access, fully independently of the VPN connection.

- Secondly, a PPTP connection is configured to the other VPN tunnel endpoint.

1.2 Prerequisites

Where to start

- If you have not yet configured an Internet connection or a WAN partner on your BinTec router, begin with section B, chapter 1.3.1, page 35.
- If you are already using your BinTec router to connect to the Internet, but have not yet configured your WAN partner, check the entries for your ISP and proceed with section B, chapter 1.3.2, page 38.

VPN license

A separate VPN license must be installed before the BinTec router will support VPN connections. If you are not sure you have one, verify the license is installed in Setup Tool's ***LICENSES*** menu.

If you do not have the VPN license yet, one can be purchased from BinTec Communications AG directly or from your local distributor.

Two BinTec routers required

A LAN-LAN VPN tunnel using BinTec´s VPN solution can only be established between two BinTec routers. It is not possible to establish a VPN connection between a BinTec router and a router from another manufacturer.

One static IP address

At least one VPN partner must have a statically configured, official IP address.

1.3 Instructions

1.3.1 Step 1: This is how to configure the connection to your ISP

The link to the ISP can be setup as a standard dial-up or as a leased-line PPP interface in the ***WAN PARTNERS*** menu.

When configuring a VPN connection over a dialup connection, it is recommended to set Short Hold for the VPN connection with a shorter time interval than the Short Hold for the underlying dial-up connection. Otherwise, unnecessary connections could be established because of termination of the VPN connection.

Adding a WAN partner

- Go to ***WAN Partner*** ➧ **ADD**.
- Enter the **Partner Name**: *ISP*.
- Select **Encapsulation**: *PPP*.
- Select **Encryption**: *none*.
- Go to **PPP**.
  The PPP submenu defines PPP settings for the partner interface.
- Select **Authentication**: e.g. ***MS-CHAP***.
- Enter **Partner PPP ID**: e.g. ***myISP***.
- Enter **Local PPP ID**: e.g. ***myBinTec***.
- Enter **PPP Password**: ****.

If you are configuring a dial-up connection, enter the WAN numbers as follows:

Dial-up connection

- Go to **WAN Numbers** ➧ **ADD**.
- Enter **WAN Number**: e.g. ***911331301***.
- Select the **Direction**: e.g. ***outgoing***.
- Go back to the ***Configure WAN Partner*** menu and then select ***IP***.

Dynamic or static IP address

Now there are two possibilities for the next setting: either your BinTec router is dynamically assigned an IP address or the IP address is statically configured.

1. If you receive your IP address dynamically:

- Select ***IP Transit Network***: *dynamic client*.
  No further settings are required on this menu page.

2. If you have a static IP address, proceed as follows:

- Select **IP Transit Network**: *yes*.

An important characteristic of the configuration concerns the following configuration points, **Local ISDN IP address** and **Partner ISDN IP address**. As you probably will not know the IP address of your ISP, only enter the official IP address of the local BinTec router in both cases.

- Under **Local ISDN IP address**, enter your own official IP address: e.g. ***198.16.13.1***.
- Under **Partner´s ISDN IP address**, also enter your own official IP address: e.g. ***198.16.13.1***.

Network Address Translation

- In the main menu, go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Select the ISP interface you have just configured and want to use NAT for.
- Activate NAT on this interface: **Network Address Translation** = *on*.

For standard, non-VPN links to the Internet, it is usually unnecessary to explicitly allow any session profiles through the NAT barrier. When the session is initiated locally and simple surfing requests are sent to the Internet, the router can identify the returning packets (by means of the source/destination IP addresses and the port number) and can reroute them back into the LAN. If, however, you have an FTP server, for example, and sessions would be initiated outside your LAN by customers wishing to download files from your server over the Internet, then it would be necessary to define session profiles in the NAT menu to allow these externally initiated sessions through your NAT barrier.

For the purposes of later allowing the construction and operation of VPN tunnels over this ISP interface, it is essential to explicitly permit the following session profiles through the NAT barrier: GRE and TCP.

Assuming the configuration of the ISP is intended to accomodate VPN tunnels.

- Press **ADD**.
- Under **Protocol** select: e.g. ***TCP***.
- Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

- Repeat for the protocol GRE and for any other protocols needed.
- Go to ***IP*** ➧ ***ROUTING*** ➧ **ADD**.

Add the default route

- Select **Route Type**: *Default route.*

Only one default route can be configured on your BinTec router and this is commonly the route to the Internet Service Provider.

- Select **Network**: *WAN without transit network*.

Another important characteristic of the configuration is that it is essential to set **Network** to *WAN without transit network* when setting the default route over the interface using NAT.

- Select **Gateway IP-Address**: *myISP*.
- Leave the menu by pressing **SAVE**.

1.3.2 Step 2: This is how to configure the VPN interface

The VPN Partner interface for your BinTec router could be configured as follows:

- Go to ***VPN*** ➧ **ADD** ➧ ***CONFIGURE VPN INTERFACES***.
- Define a partner name.
- In the **Encryption** field, you may select *MPPE* (*40*-bit or *128*-bit session-key) or *none*. The options specified here must be the same for each partner.
- Go to the ***PPP*** submenu.

The following menu opens:

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD][PPP]: PPP Settings (H.Q.)                            MyRouter


Authentication                          MS-CHAP
Partner PPP ID                          HQ-ppp-id
Local PPP ID                            mybrick
PPP Password                            *******

Keepalives                              on
Link Quality Monitoring                 off

                    SAVE                    CANCEL

Use <Space> to select
```

➤ In the **Authentication** field, select which authentication to use.

If MPPE 128 was selected, the MS-CHAP protocol is required here.

➤ Set **Partner PPP ID** and **PPP Password** as needed.

In the ***IP*** menu you will need to define the IP addresses the VPN Partner will be using.

```
BRICK Setup Tool                               BinTec Communications AG
[VPN][ADD][IP]: IP Configuration (H.Q.)                          MyRouter


VPN Partner's IP Address                198.16.13.1
via IP Interface                        ISP
Identification by IP Address            yes

local IP Address

Partner's LAN IP Address                10.5.5.0
Partner's LAN Netmask                   255.255.255.0

Advanced Settings>

                SAVE                    CANCEL

Enter string, max length = 25 chars
```

- Enter the official IP address of your partner after **VPN Partner's IP Address**: e.g. ***198.16.13.1***.
- Under **via IP Interface** select the PPP interface for the local ISP. VPN connections from this side may only be established over this interface.
- Even if you do not know the **VPN Partner's IP Address** above, enable (*yes*) the **Identification by IP Address** option. If you have entered **VPN Partner's IP Address**, the VPN partner will be identified by the IP address it uses when establishing the PPP link.
- No entry is necessary for **local IP Address**.
- Specify LAN address and netmask in the **Partner's LAN IP Address/Netmask** fields.

If you did not already do so in the previous step (section B, chapter 1.3.1, page 35), it is now imperative for the success of your VPN tunnel that you define two session profiles that may be permitted through the NAT barrier. This means that sessions initiated by the other side of the VPN can pass the NAT firewall and access your LAN.

The session profiles should be set on the ISP interface, not the VPN interface.

Network Address Translation

- In the main menu, go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Select the ISP interface you configured.
  Network Address Translation should be already activated on this interface.
- Press **ADD**.
- Under **Protocol** select: *tcp*.
- Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

- Leave the menu by pressing **SAVE**.
  You will see the TCP entry listed.
- Press **ADD**.

- Under **Protocol** select: *gre*.
- Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

- Leave the menu by pressing **SAVE**.

  You will see the TCP and GRE entries listed.

This completes the basic cycle of settings required to establish LAN-to-LAN VPN connections. To ensure the success of your configuration, you can now test the tunnel in the following section.

1.4 Testing and Trouble Shooting

1.4.1 Testing your VPN connection

- from a host in your LAN, ping a host in the partner LAN or
- if you want to test from a BinTec router to a partner BinTec router, enter the BinTec router's LAN IP address as **Unique Source IP Address** in Setup Tool menu ***IP*** ➧ ***STATIC SETTINGS*** before testing. Otherwise, the BinTec router will put the IP address of the WAN interface as source address into the ping packets originated by the BinTec router with the result being that outgoing packets to the VPN partner are sent through the tunnel, but can only be returned outside the tunnel (on the underlying WAN connection).

1.4.2 BinTec test access

If you are still having problems establishing a VPN tunnel, you can follow a step by step configuration which will lead you to a BinTec test access site. This can be found in the form of an FAQ on the support pages of www.bintec.de. Once you have achieved this test access, compare and exchange the values you need for your own VPN tunnel.

2 How Do I Configure and Connect a LAN-to-LAN VPN with Callback

2.1 Introduction

Let´s assume in this example that only ***headquarters*** has a statically configured official IP address. ***Sales office*** receives its IP address dynamically from its ISP. Therefore, only ***sales office*** can initiate the VPN connection. ***Headquarters***, however, needs VPN connections to be periodically established in order to transmit mails from a central mail server to the ***sales office***. Without actively establishing the tunnel, it can trigger the process with the Callback function.

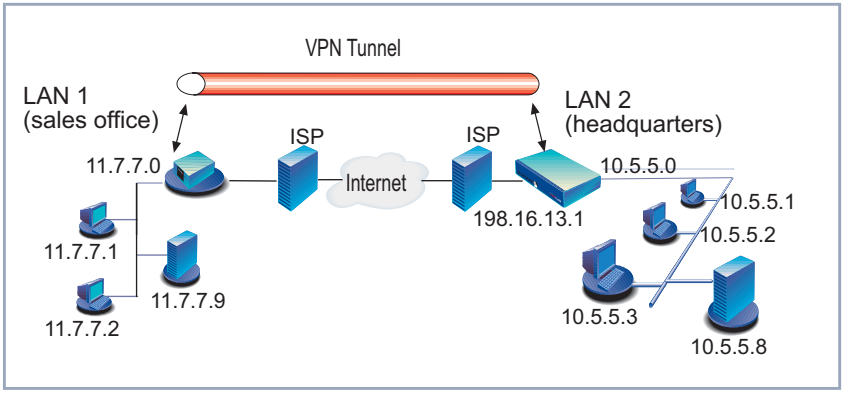

Figure B-2: LAN-to-LAN configuration example

The Configuration

Essentially the configuration is the same as in the example in section B, chapter 1.1, page 34, the instructions below will supplement this configuration with a few additional settings necessary for the success of the Callback function.

Essentially, these additional settings are configured in four stages:

- Firstly, on the router at ***headquarters*** it is necessary to configure a new WAN partner entry for your VPN partner (***sales office***) over Setup Tool

over which Callback will take place. A second interface with the same IP route destination is thus created.

- The existing VPN interface entry is then configured with a higher metric so that all connections made from this side (***headquarters***) are made over this newly configured dialup interface.
- Thirdly, the receiving end (***sales office***) must be configured to identify the call intended to trigger Callback.
- Lastly, Callback must be activated on the VPN interface of the side that should actively establish the VPN connection (***sales office***).

2.2 Prerequisites

Experience with MIB tables

Setup Tool will always cover the most essential parts of a configuration. There are, however, some few areas of a total configuration where subtle solutions to more complex, network-management issues can only be managed over MIB tables. The MIB tables allow the user to fine-tune a configuration. Changes to MIB variables should only be made by experienced professionals who understand the implications of each setting. The Callback feature can only be configured by means of the MIB tables.

Existing tunnel

The instructions below presuppose a properly configured and functional Virtual Private Network. If you have not yet configured the basic settings for your VPN, read the appropriate Workshop for your scenario (section B, chapter 1.1, page 34 or section B, chapter 3, page 48), configure accordingly and then return here for the configuration of the Callback feature.

2.3 Instructions

2.3.1 This is how to configure a LAN-to-LAN VPN with Callback

Configuration on headquarters

- Go to ***WAN PARTNER*** ➧ **ADD**.

Adding a WAN partner over Setup Tool

- Enter the **Partner Name**: sales.
- Select **Encapsulation**: *PPP*.
- Select **Encryption**: *none*.
- Go to **PPP**.
  The PPP submenu defines PPP settings for the partner interface.
- Select **Authentication**: e.g. ***MS-CHAP***.
- Enter **Partner PPP ID**: e.g. ***sales_nbg***.
- Enter **Local PPP ID**: e.g. ***myBinTec***.
- Enter **PPP Password**: ****.
- Go to **WAN Numbers** ➧ **ADD**.
- Enter **WAN Number** of WAN partner (sales office): e.g. ***911331301***.
- Select the **Direction**: e.g. ***outgoing***.
- Go back to the ***CONFIGURE WAN PARTNER*** menu and then select ***IP***.
- Under **Partner´s LAN IP Address**, enter the LAN IP address of your VPN partner, in the example: 11.7.7.0.
- Under **Partner´s LAN Netmask**, enter the LAN IP address of your VPN partner, in the example: 255.255.255.0.

2 Routes, 1 Destination

Now there are two entries in the **ipRouteTable** routed to the same destination: the initial virtual interface route and a route to the same destination over which Callback will be triggered. In order to ensure the "trigger route" will be used

when contacting the partner, it is necessary to increase the metric of the virtual interface by a value of 1.

```
bintec:ipRouteTable>Metric1:02=2
02: ipRouteTable1.0.0.0.0.2(rw):2
bintec:ipRouteTable>

inxDest(*rw)     IfIndex(rw       Metric1(rw)      Metric2(rw)
   Metric3       Metric4(rw)      NextHop(rw)      Type(-rw)
   Proto(ro)     Age(rw)          Mask(rw)         Metric5(rw)

02 11.7.7.0      10001            2                -1
   -1            2                0.0.0.0          indirect
   local         257610           255.255.255.0    536870912

04 11.7.7.0      10002            1                -1
   -1            2                0.0.0.0          indirect
   local         257612           255.255.255.0    536870912
   .0.0

bintec:ipRouteTable>
```

VPN interface

Dialup interface

Table B-1: **ipRouteTable**

Configuration on sales office

Identifying the dialup connection

Now it is necessary to tell ***sales office*** about the dialup interface being used to initiate Callback. Using the VPN interface index, an entry must be made in the **biboDialTable** of ***sales office*** in which **biboDialDirection** is set to *incoming* and **biboDialNumber** is set with the Calling Party´s Number, i.e. the ISDN phone number of ***headquarters***.

```
bintec:biboDialTable>Direction:01=incoming Number:01=983641
01:   biboDialDirection.10002.9(rw):both
01:   biboDialNumber.10002.9(rw):   "983641"
bintec:biboDialTable>

inxIfIndex(ro)       Type(*rw)            Direction(rw)
   Number(rw)        Subaddress(rw)       ClosedUserGroup(rw)
   StkMask(rw)       Screening(rw)

00 10001             isdn                 outgoing
   "432958"                               0
   0xffffffff        dont_care
```

DialTable entry for ISP

DialTable entry for VPN

DialTable entry for Call-back trigger

```
01 10002              isdn                  both
   198.16.13.1                              0
   0xffffffff         dont_care

02 10002              isdn                  incoming
   "983641"                                 0
   0xffffffff         dont_care

bintec:biboDialTable>
```

Table B-2: **biboDialTable**

Configuring Callback

Finally, it is necessary to configure the VPN interface to Callback *delayed* in the **biboPPPTable** on the ***sales office*** router.

Once ***sales office*** receives the Callback trigger call from ***headquarters***, it will close this initial connection (no charges are incurred) and establish the desired tunnel to its ***headquarters***.

```
bintec:biboPPPTable>Callback:01=delayed
01:biboppCallback.1.19(rw):  delayed
bintec:biboPPPTable>biboPPPTable

inxIfIndex(ro)        Type(*rw)             Encapsulation(-rw)
Keepalive(rw)         Timeout(rw)           Compression(rw)
Authentication(rw)    AuthIdent(rw)         AuthSecret(rw)
IpAddress(rw)         RetryTime(rw)         BlockTime(rw)
MaxRetries(rw)        ShortHold(rw)         InitConn(rw)
MaxConn(rw)           MinConn(rw)           Callback(rw)
Layer1Protocol(rw)    LoginString(rw)       VJHeaderComp(rw)
Layer1Mode(rw)        DynShortHold(rw)      LocalIdent(rw)
DNSNegotiation(rw)    Encryption(rw)        LQMonitoring(rw)
IpPoolId(rw)
```

ISP interface

```
00 10001              isdn_dialup          ppp
   off                3000                 none
   both
   static             4                    300
   5                  60                   1
   1                  1                    disabled
   data_64k                                disabled
   auto               0
   enabled            none                 off
   0
```

VPN interface

```
01 10002              isdn_dialup          ppp
   off                3000                 none
   both
   static             4                    300
   5                  30                   1
   1                  1                    delayed
   pptp_pns                                disabled
   auto               0
   enabled            none                 off
   0

bintec:biboPPPTable>
```

Table B-3: **biboPPPTable**

3 How Do I Configure and Connect a Client-to-LAN VPN

3.1 Introduction

The Virtual Private Network scenario outlined above in Technology Overview, section A, chapter 1.6.3, page 21, would be configured as described in this chapter.

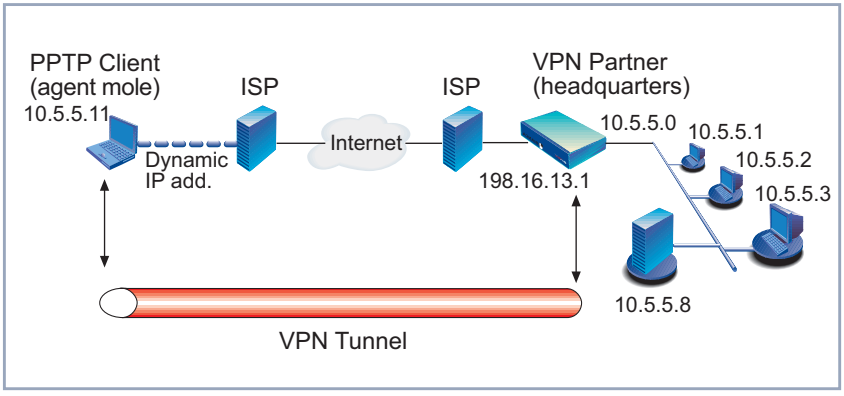

Figure B-3: A typical client-to-LAN scenario.

There are essentially four configuration stages to be considered:

Client-side

- The first thing to do is to configure the PPP client. Here it is necessary to enter the settings required to establish the PPP link to the Internet Service Provider.
- Once that is done, the next step will be to configure a PPTP link from the client to a BinTec VPN server.

LAN-side

- The third stage involves a basic configuration of your BinTec router to connect to its ISP.
- The final stage entails configuring the VPN interface on your BinTec router.

3.2 Prerequisites

Client-side: TCP/IP & PPTP protocol

For the type of tunneling described in this chapter, two network protocols must be installed: TCP/IP and PPTP. TCP/IP is supported on all Windows operating systems since Windows 95. Under Windows 95, however, a software update for the PPTP protocol is required.

This upgrade under the title "Dial-Up Networking 1.2 Upgrade", as well as additional configuration information can be retrieved from Microsoft's web site at: http://www.microsoft.com

This description is based on Windows NT, no update for the PPTP protocol is required. The Point-to-Point Tunneling Protocol (PPTP), however, must be installed and RAS devices configured. The following is a brief explanation of how to install the PPTP protocol and how to configure the RAS devices.

Installing the PPTP protocol

- Click **Start**, point to **Settings**, and then click **Control Panel**.
- Double-click **Network**.
- Select the **Protocols** tab, and then click **Add** to display the **Select Network Protocol** dialog box.
- Select **Point To Point Tunneling Protocol**, and then click **OK**.
- Type the drive and directory location of your installation files in the **Windows NT Setup** dialog box, and then click **Continue**.
- Select the **Number of Virtual Private Networks** the client will support. One is usually enough.

The number of VPNs selected here will be offered as **RAS Capable Devices** when configuring Remote Access Service devices in the next step.

- Click **OK**, and then **OK** once again.

Configuring a VPN device on the client

Now that PPTP is installed, it is necessary to add a VPN device (**VPN1 - RASPPTPM**) or devices to the Remote Access Service (RAS).

- In the following window, click **Add** to add a VPN device.

If you don´t arrive at **Add RAS Device** directly after installing PPTP,

- click **Start**, point to **Settings**, click **Control Panel**.
- double-click **Network**.
- select the **Services** tab, and then click **Remote Access Service**.
- click **Properties** to display the **Remote Access Setup** properties page.
- then click **Add**.

- Select in the drop-down list **VPN1 - RASPPTPM**.

In addition to adding a VPN device, it is necessary that a modem or ISDN card is also installed to enable basic connections to the Internet Service Provider. If this has not yet been done, click the **Install Modem** button in the **Add RAS Device** page and follow the instructions.

- Click **OK**.
- In **Remote Access Setup**, select a VPN port and click **Configure**.
- Assuming this client receives its IP address dynamically, ensure that the **Dial out only** option in the **Port Usage** dialog box is selected.
- Click **OK.**

  You have returned to the **Remote Access Setup** page.
- Click **Network** and ensure that **TCP/IP** is selected as the **Dial out Protocol** in the **Network Configuration** dialog box.
- Click **OK.**

  You have returned to the **Remote Access Setup** page.
- Click **Continue**.
- On the **Network** page, click **Close**.
- Restart your computer.

Two dial-up networking entries

When PPTP is installed and configured as a RAS device on the Windows client, two **Dial-Up Networking** entries are required on that client: one for the ISP and one for the VPN partner network. These configuration steps are described in the instructions in section B, chapter 3.3, page 51.

LAN-side: VPN license A separate VPN license must be installed before the BinTec router will support VPN connections. A VPN license can be purchased from your local distributor.

One static IP address As the client will probably receive its IP address dynamically from the ISP, the LAN partner participating in the VPN must have a statically configured, official IP address.

3.3 Instructions

3.3.1 Step 1: This is how to configure a PPP link from a Windows NT host to an ISP

➤ Open the **Dial-Up Networking** folder by double-clicking **My Computer** from the desktop, and then **Dial-Up Networking**.

The following windows open:

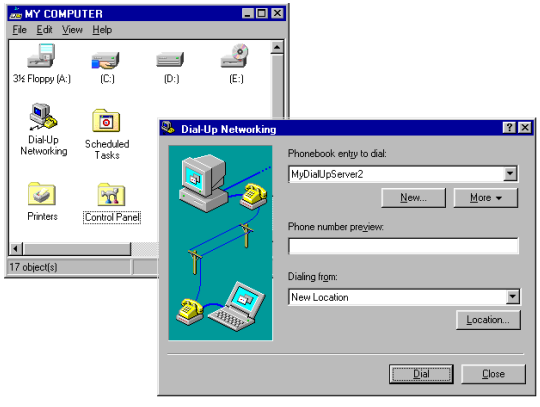

Figure B-4: **Dial-up Networking**

➤ Click the **New** button.

The **New Phonebook Entry** wizard appears

➤ Under **Entry Name** in the resulting dialog box, specify a name for the ISP this host will be using.

➤ Under **Phone number**, you will need to enter the ISP's telephone number.

- Under **Dial using**, select from the drop-down list a modem device you will be using to connect with your Internet Service Provider.
- Click the **Server** tab.

The following window opens:

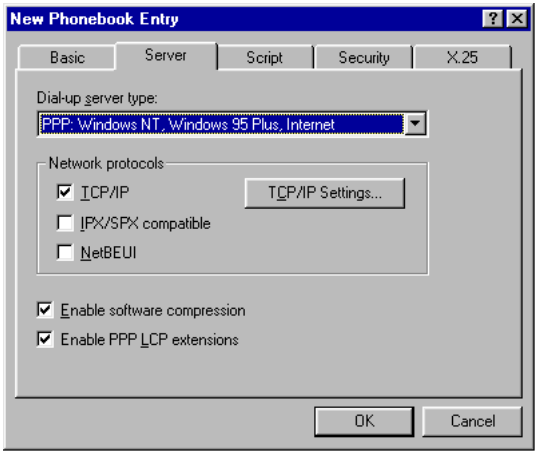

Table B-4: Internet Service Provider

- In the **Dial-up server type** field, select: **PPP: Windows NT, Windows 95 Plus, Internet.**
- In the **Network protocols** box: verify **TCP/IP** is enabled, **NetBEUI** is disabled and **IPX** is disabled.
- Ensure the **Enable software compression** and **Enable PPP LCP extensions** match the configurations on the partner VPN.
- Click the **TCP/IP Settings...** button. Verify the IP address, name service, and compression settings are consistent with those required by the ISP and click **OK**.

In most cases, the default settings in the **Script** and the **X25** tabs can be left untouched.

- Click the **Security** tab.

- Check the kind of authentication specified by your ISP.
- Click **OK** again. The initial PPP link to the Internet Service Provider is now configured.
  Proceed to the next section to configure another dial-up networking entry, this time a virtual interface to your VPN partner using PPTP.

3.3.2 Step 2: This is how to configure the PPTP link from the Client to the BinTec router

- Open the **Dial-Up Networking** folder by double-clicking **My Computer** from the desktop, and then **Dial-Up Networking**.
- Click the **New** button.

The **New Phonebook Entry** wizard opens:

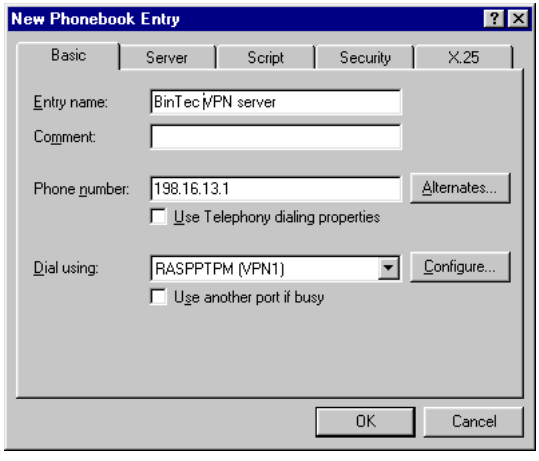

Figure B-5: **New Phonebook Entry** wizard

- Under **Entry Name**, specify a name for the VPN partner this host will be using.
- Under **Phone number**, you will need to enter the official IP address of the VPN server on the other side.
- Clear the **Use telephony dialing properties** check box.

- Under **Dial using**, select **VPN1 - RASPPTPM** from the drop-down list.
- Clear the **Use another port if busy** check box.
- Click the **Server** tab.
- In the **Dial-up server type** field select: **PPP: Windows 95, Windows NT, Internet**.
- In the **Network protocols** box: verify **TCP/IP** is enabled, **NetBEUI** is disabled and **IPX** is disabled.
- The **Enable software compression** and **Enable PPP LCP extensions** settings used here must correspond to the respective BinTec router VPN partner interface settings (see section B, chapter 3.3.4, page 57).

In most cases, the default settings in the **Script** and the **X25** tabs can be left untouched.

- Click the **TCP/IP Settings...** button. Verify the IP address, name service, and compression settings are consistent with those required by your VPN partner and click **OK**.
- Click the **Security** tab.

The following window opens:

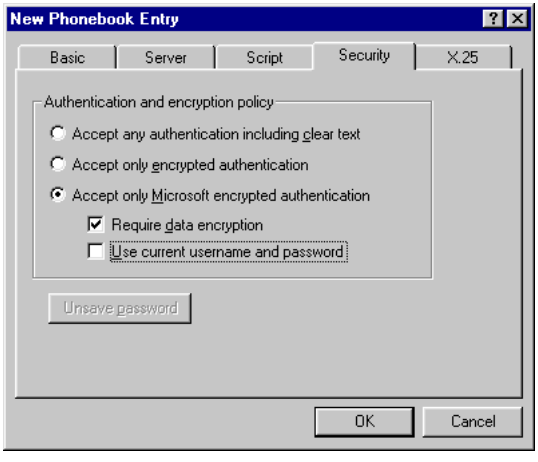

Figure B-6: **Security** tab

- Check **Accept only Microsoft encrypted authentication** and then **Require data encryption**.
- Click **OK** again to accept the settings for the PPTP link.
  Once the respective BinTec router interfaces are configured, the Virtual Private Networking connection can be established as described in section B, chapter 3.4, page 61.

3.3.3 Step 3: This is how to configure a connection from a BinTec router to an ISP

Now to the other side of the VPN link and to Setup Tool on the BinTec router.

The link to the ISP can be set up as a standard dial-up or as a leased-line PPP interface in the ***WAN PARTNERS*** menu.

Adding a WAN partner: LAN-side

- Go to ***WAN PARTNER*** ➧ **ADD**.
- Enter the **Partner Name**: *ISP*.
- Select **Encapsulation**: *PPP*.
- Select **Encryption**: *none*.
- Go to **PPP**.
  The PPP submenu defines PPP settings for the partner interface.
- Select **Authentication**: e.g. ***MS-CHAP***.
- Enter **Partner PPP ID**: e.g. ***myISP***.
- Enter **Local PPP ID**: e.g. ***myBinTec***.
- Enter **PPP Password**: ****

If you are configuring a dial-up connection:

- Go to **WAN Numbers** ➧ **ADD**.
- Enter **WAN Number**: e.g. ***911331301***.
- Select the **Direction**: e.g. ***outgoing***.

➤ Go back to the ***CONFIGURE WAN PARTNER*** menu and then select ***IP***.

Assuming the client receives its IP address dynamically, the BinTec router must have a statically configured, official IP address. Therefore, proceed as follows:

➤ Select **IP Transit Network**: *yes*.

An important characteristic of the configuration concerns the following configuration points, **Local ISDN IP address** and **Partner ISDN IP address**. As you probably will not know the IP address of your ISP, only enter the official IP address of the local BinTec router in both cases.

➤ Under **Local ISDN IP address**, enter your own official IP address: e.g. ***198.16.13.1***.

➤ Under **Partner ISDN IP address**, also enter your own official IP address: e.g. ***198.16.13.1***.

Network Address Translation

➤ In the main menu, go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

➤ Select the ISP interface you have just configured and want to use NAT for.

➤ Activate NAT on this interface: **Network Address Translation** = *on*.

For standard, non-VPN links to the Internet, it is usually unnecessary to explicitly allow any session profiles through the NAT barrier. When the session is initiated locally and simple surfing requests are sent to the Internet, the router can identify the returning packets and can reroute them back into the LAN. If, however, you have an FTP server, for example, and sessions would be initiated outside your LAN by customers wishing to download files from your server over the Internet, then it would be necessary to define session profiles in the NAT menu to allow these sessions through your NAT barrier.

For the purposes of later allowing the construction and operation of VPN tunnels over this ISP interface, it is essential to explicitly permit the following session profiles through the NAT barrier: GRE and TCP.

Assuming the configuration of the ISP is intended to accomodate VPN tunnels:

➤ Press **ADD**.

➤ Under **Protocol**, select *TCP*.

➤ Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

➤ Repeat for the protocol GRE and for any other protocols needed.

➤ Go to ***IP*** ➧ ***ROUTING*** ➧ **ADD**.

Add the default route

➤ Select **Route Type**: *Default route*.

Only one default route can be configured on your BinTec router and this is commonly the route to the Internet Service Provider.

➤ Select **Network**: *WAN without transit network*.

Another important characteristic of the configuration is that it is essential to set **Network** to *WAN without transit network* when setting the default route over the interface using NAT.

➤ Select **Gateway IP-Address**: *myISP*.

➤ Leave the menu by pressing **SAVE**.

3.3.4 Step 4: This is how to configure the VPN interface on your BinTec router

The VPN Partner interface for your BinTec router could be configured as follows:

➤ Go to ***VPN*** ➧ **ADD** ➧ ***CONFIGURE VPN INTERFACES***.

The following menu opens:

```
BinTec Setup Tool                                BinTec Communications AG
[VPN][ADD]: Configure VPN Interfaces                              MyRouter

Partner Name                          H.Q.

Encapsulation                         PPP
Compression                           none
Encryption                            MPPE 128


PPP>
Advanced Settings>

IP >
IPX >


                     SAVE                 CANCEL

Enter string, max length = 25 chars
```

- Define a partner name.
- In the **Encryption** field, select the option agreed upon by both sides of the VPN.
- Go to the ***PPP*** submenu.

The following menu opens:

```
BRICK Setup Tool                                 BinTec Communications AG
[VPN][ADD][PPP]: PPP Settings (Agent mole)                        MyRouter



Authentication                    MS-CHAP
Partner PPP ID                    mole-ppp-id
Local PPP ID                      myrouter
PPP Password                      *******

Keepalives                        off
Link Quality Monitoring           off


                OK                        CANCEL

Use <Space> to select
```

- In the **Authentication** field, select which authentication to use.

The **Authentication** entry here must match the entry for the *AuthProtocol* variable in the **biboPPPProfileTable**.

If MPPE 128 was the encryption protocol selected, the MS-CHAP protocol is required here.

➤ Set **Partner PPP ID** and **PPP Password** as needed.

In the ***IP*** submenu, you will need to define the IP addresses the VPN Partner will be using:

```
BRICK Setup Tool                              BinTec Communications AG
[VPN][ADD][IP]: IP Configuration (Agent mole)                 MyRouter


VPN Partner's IP Address

Identification by IP Address          no

local IP Address

Partner's LAN IP Address              10.10.5.11
Partner's LAN Netmask                 255.255.255.255
Advanced Settings>

                 SAVE                 CANCEL

Enter string, max length = 25 chars
```

➤ As your VPN partner is probably a dial-in client and is assigned its IP address dynamically, you will not know the **VPN Partner's IP Address**.

➤ Disable (*no*) the **Identification by IP Address** option. The VPN partner will not be identified by the IP address it uses when establishing the PPP link. It cannot be if it is a dynamic client.

➤ Enter the **Partner's LAN IP Address** and **Netmask**.

➤ If, as is often the case, the partner is using a LAN address from the network of the headquarters, it is necessary to activate **Proxy Arp**.

➤ Go to ***VPN*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

The following menu opens:

```
BinTec Setup Tool                              BinTec Communications AG
[VPN][ADD][IP][ADVANCED]: Advanced Settings (Agent Mole)      MyRouter

RIP Send                                       none
RIP Receive                                    none

Dynamic Name Server Negotiation                no

IP Accounting                                  off
Back Route Verify                              off
Route Announce                                 up or dormant
Proxy Arp                                      off

                          OK                       CANCEL

Use <Space> to select
```

- If the partner is using a LAN address from the network of the headquarters, configure **Proxy Arp** to *on (up only)*.

If you did not already do so in the previous step (section B, chapter 3.3.3, page 55), it is now imperative for the success of your VPN tunnel that you define two session profiles that may be permitted through the NAT barrier. This means that sessions initiated by the other side of the VPN can pass the NAT firewall and access your LAN.

The session profiles should be set on the ISP interface, not the VPN interface.

Network Address Translation

- In the main menu (section A, chapter 2.1, page 23), go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Select the ISP interface you configured.

Network Address Translation should be already activated on this interface.

- Press **ADD**.
- Under **Protocol**, select *tcp*.
- Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

- Leave the menu by pressing SAVE.
  You will see the TCP entry listed.
- Press **ADD**.
- Under **Protocol** select: *gre*.
- Under **Destination**, you have to specify the router as tunnel endpoint.

The loopback address, 127.0.0.1, should be used as the destination address. Assigned to the BinTec router itself, this address is the recommended destination as the BinTec router is an endpoint of the VPN tunnel

- Leave the menu by pressing SAVE.
  You will now see the TCP and GRE entries listed.

This completes the basic cycle of settings required to establish VPN connections from a client to a LAN partner. To ensure the success of your configuration, you can now test the tunnel in the following section.

3.4 Testing & Trouble Shooting

3.4.1 Testing your configuration

From the perspective of the client, this is how to test the connection to the BinTec router and the success of your VPN tunnel.

Establishing a PPP link to the ISP

- Open the **Dial-Up Networking** folder by double-clicking **My Computer**, and then **Dial-Up Networking**.

The following window opens:

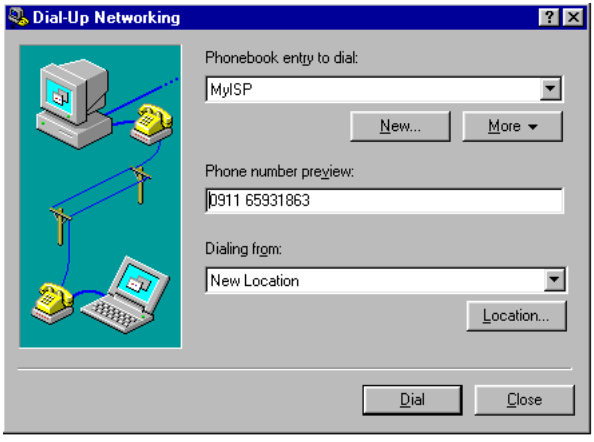

Figure B-7: **Dial-Up Networking**

- Click **Dial**.
- In the **Connect to MyISP** dialog box, enter the **User name** and **Password** assigned by the ISP.

The following window opens:

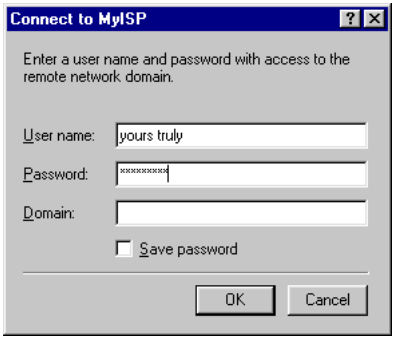

Figure B-8: **User Name** and **Password**

Establishing a PPTP link to the BinTec router

- After connecting to the ISP, select the BinTec VPN server **Phonebook entry to dial** in the **Dial-up Networking** dialog box and click **Dial**.

The following window opens:

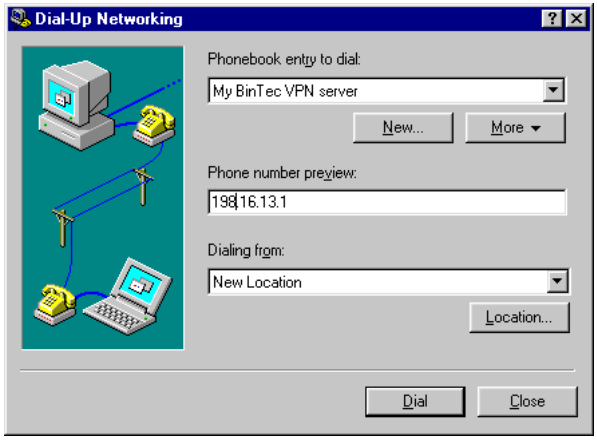

Figure B-9: **Phonebook entry to dial**

- In the **Connect To My BinTec VPN server** window shown below, enter the PPP ID and PPP Password settings configured on the BinTec router in the **User name** and **Password** fields and press **OK**.

The following window opens:

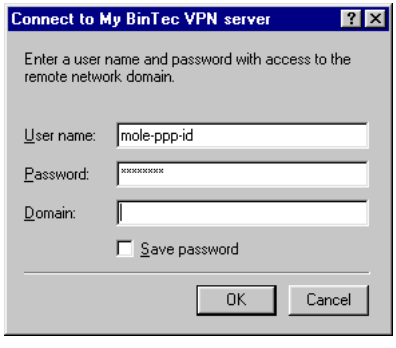

Figure B-10: PPP ID and PPP Password

3.4.2 Tracing errors

If the VPN tunnel could not be established and a data exchange was not possible, narrow down the possible areas of misconfiguration.

- To test the ISP connection from a workstation behind your BinTec router, simply ping the IP address of an Internet site such as 195.185.6.70 (BinTec´s web server).
- To test the ISP connection from your client PC, ping the IP address of an Internet site such as 195.185.6.70 (BinTec´s web server).
- To ensure that essential parameters are consistent between both sides, try to establish a normal PPP connection to your WAN partner.

If the destination host proves unreachable in any of these stages, review the settings made for that part of the configuration.