PPTP

Bintec User’s Guide - VPN Access Series
Version 1.0

Purpose

This document is part of the user's guide to the installation and configuration of Bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.bintec.net.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for Bintec gateways can be found at www.bintec.net.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

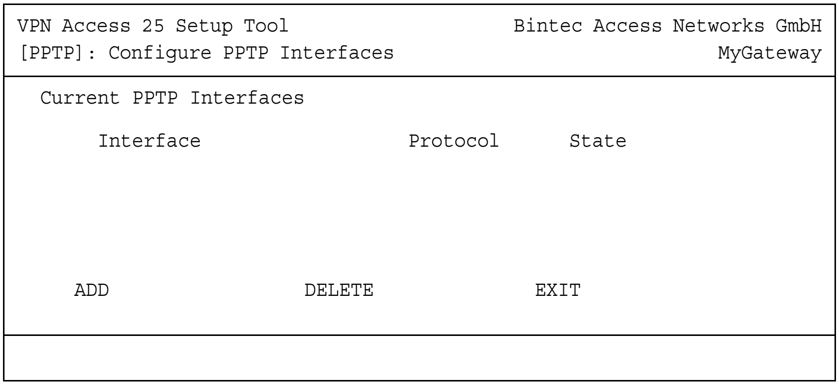
You will find detailed information in the Declarations of Conformity at www.bintec.net.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 PPTP Menu

The fields of the *PPTP* menu are described below.



```
VPN Access 25 Setup Tool                         Bintec Access Networks GmbH
[PPTP]: Configure PPTP Interfaces                                  MyGateway

  Current PPTP Interfaces

       Interface                       Protocol      State




     ADD                  DELETE                EXIT
```

The Point-to-Point Tunneling Protocol (=PPTP) can be used to set up an encrypted PPTP tunnel to provide security for data traffic over an existing IP connection.

Setting up a tunnel

First a connection to an ISP (=Internet Service Provider) is set up at both sites. Once these connections are available, a tunnel is set up to the PPTP partner over the Internet using PPTP.

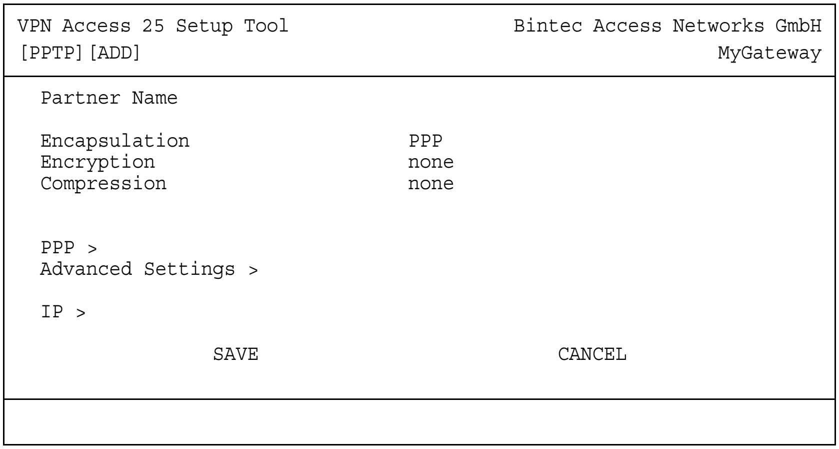
Control connection

The PPTP subsystem sets up a control connection between the endpoints of the tunnel. This is used to transfer control data for setting up, maintaining and terminating the connection between the two endpoints of the PPTP tunnel.

Traffic flow

As soon as this control connection is set up, the PPTP transfers the traffic data packed in GRE packets (GRE = Generic Routing Encapsulation).

The PPTP interfaces are configured in the ***PPTP*** ➜ ***ADD/EDIT*** menu.



```
VPN Access 25 Setup Tool                   Bintec Access Networks GmbH
[PPTP][ADD]                                                  MyGateway

  Partner Name

  Encapsulation                    PPP
  Encryption                       none
  Compression                      none


  PPP >
  Advanced Settings >

  IP >

               SAVE                          CANCEL

```

The menu consists of the following fields:

Field	Description
Partner Name	Enter a name for uniquely identifying the PPTP partner. The first character in this field must not be a number and no special characters or umlauts are to be used either. The maximum length is limited to 25 characters.
Encapsulation	The encapsulation method to be used. Only PPP is possible at present.
Encryption	Defines the data encryption method to be used. Possible values: see “Encryption selection options” on page 6.

Field	Description
Compression	Defines the compression to be used and is only active if the remote terminal has a similar configuration. Possible values: ■ *none* (default value): No compression ■ *STAC*: STAC data compression (to RFC 1974, 1967) ■ *MS-STAC*: Microsoft variant of STAC data compression ■ *MPPC*: Microsoft Point-to-Point Compression A combination of encryption and compression is only possible with (any) MPPE encryption and MPPC. The free license necessary for using STAC and MPPC can be obtained from the service section of www.bintec.net.

Table 1-1: ***PPTP*** menu fields

ENCRYPTION offers the following selection options:

Description	Meaning
none (default value)	No encryption
MPPE 40	MPPE version 1 and 2 with 40-bit key
MPPE V2 40	MPPE version 2 with 40-bit key
MPPE V2 40 (RFC 3078)	MPPE version 2 with 40-bit key as per RFC 3078: for Microsoft clients with Windows 2000 or later (with Service Packs as applicable)
MPPE V1 40 only	MPPE version 1 with 40-bit key
MPPE 56	MPPE version 1 and 2 with 56-bit key
MPPE V2 56	MPPE version 2 with 56-bit key

Description	Meaning
MPPE V2 56 (RFC 3078)	MPPE version 2 with 56-bit key as per RFC 3078: for Microsoft clients with Windows 2000 or later (with Service Packs as applicable)
MPPE V1 56 only	MPPE version 1 with 56-bit key
DES 56	DES with 56-bit key
Blowfish 56	Blowfish with 56-bit key
MPPE 128	MPPE version 1 and 2 with 128-bit key
MPPE V2 128	MPPE version 2 with 128-bit key
MPPE V2 128 (RFC 3078)	MPPE version 2 with 128-bit key as per RFC 3078: for Microsoft clients with Windows 2000 or later (with Service Packs as applicable)
MPPE V1 128 only	MPPE version 1 with 128-bit key
MPPE V1 128 (MS-compatible mode)	Microsoft-compatible MPPE version 1 with 128-bit key for MS-CHAP V1 authentication (not conforming to RFC 3079)
MPPE V2 128 (MS-compatible mode)	Microsoft-compatible MPPE version 2 with 128-bit key for MS-CHAP V1 authentication (not conforming to RFC 3079)
DES3 168	Triple DES with 168-bit key
Blowfish 168	Blowfish with 168-bit key

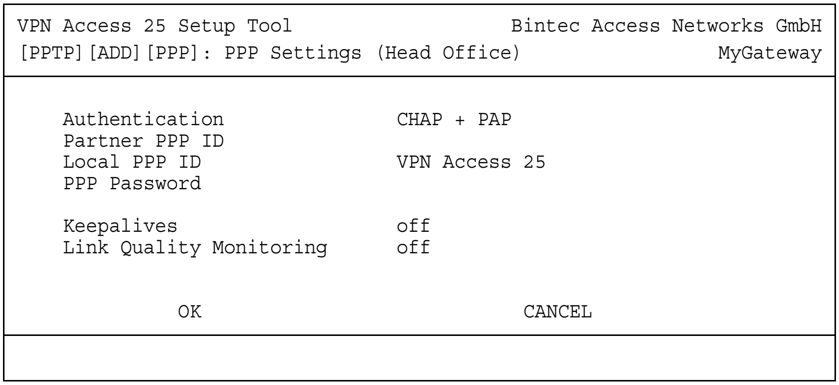
Table 1-2: ***ENCRYPTION*** selection options

The menu also provides access to the following submenus:

- ***PPP***
- ***ADVANCED SETTINGS***
- ***IP***
- ***WAN NUMBERS***: Only if ***CALLBACK*** = *yes (callback via PPTP VPN)*.

2 PPP Submenu

The *PPP* submenu is described below.



```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[PPTP][ADD][PPP]: PPP Settings (Head Office)                        MyGateway


    Authentication                 CHAP + PAP
    Partner PPP ID
    Local PPP ID                   VPN Access 25
    PPP Password

    Keepalives                     off
    Link Quality Monitoring        off


              OK                              CANCEL
```

The ***PPTP* ➜ *ADD/EDIT* ➜ *PPP*** submenu is used for making specific ➤➤ **PPP** settings for the respective PPTP partner interface. These settings are used by the gateway for authentication negotiation with the remote terminal.

The ***PPP*** menu consists of the following fields:

Field	Description
Authentication	Authentication Protocol Possible values: see “Selection options in Authentication field” on page 9
Partner PPP ID	ID of PPTP partner
Local PPP ID	ID of your gateway The default value is the entry for ***LOCAL PPP ID*** in the ***SYSTEM*** menu.
PPP Password	Password

Field	Description
Keepalives	Setting of the PPP Keepalive function for checking the reachability of the PPP remote terminal. Possible values: ■ *off* (default value) - deactivates Keepalive. ■ *on* - activates Keepalive. The PPP Keepalive function sends a packet to the remote terminal every three seconds. If the packet remains unanswered five times, the interface is set to *dormant*.
Link Quality Monitoring	Activates PPP Link Quality Monitoring as per RFC 1989. Possible values: ■ *off* (default value) ■ *on:* only necessary in exceptional cases

Table 2-1: ***PPP*** menu fields

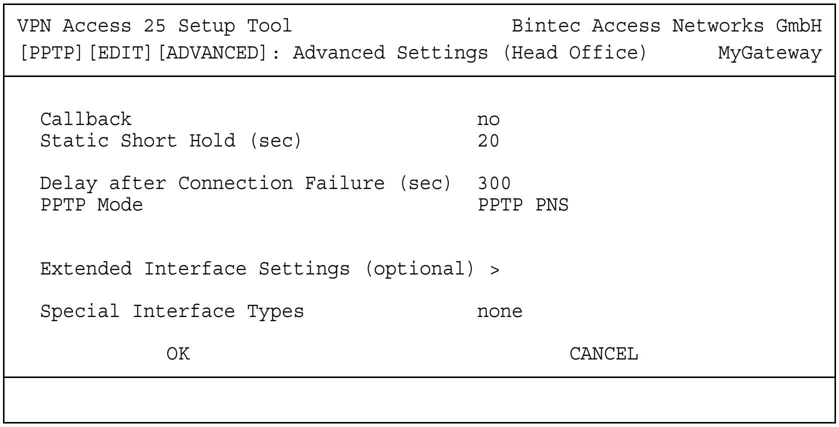
The ***Authentication*** field contains the following selection options:

Description	Meaning
PAP	Only run ➤➤ **PAP** (Password Authentication Protocol); the password is transferred unencrypted.
CHAP	Only run ➤➤ **CHAP** (Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted.
CHAP + PAP (Default value)	Run primarily CHAP, otherwise PAP.
MS-CHAP	Only run MS-CHAP version 1 (Microsoft Challenge Handshake Authentication Protocol).
CHAP + PAP + MS-CHAP	Run primarily CHAP, if denied then the authentication protocol required by the WAN partner (MS-CHAP version 1 or 2 possible).
MS-CHAP V2	Run MS-CHAP version 2 only.
none	Run no PPP authentication protocol.

Table 2-2: Selection options in ***Authentication*** field

3 Advanced Settings Submenu

The *ADVANCED SETTINGS* submenu is described below.



```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[PPTP][EDIT][ADVANCED]: Advanced Settings (Head Office)          MyGateway

  Callback                                      no
  Static Short Hold (sec)                       20

  Delay after Connection Failure (sec)          300
  PPTP Mode                                     PPTP PNS


  Extended Interface Settings (optional) >

  Special Interface Types                       none

           OK                                          CANCEL
```

The settings in the ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** menu are used to define other individual properties of the PPTP partner.

The ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** menu consists of the following fields:

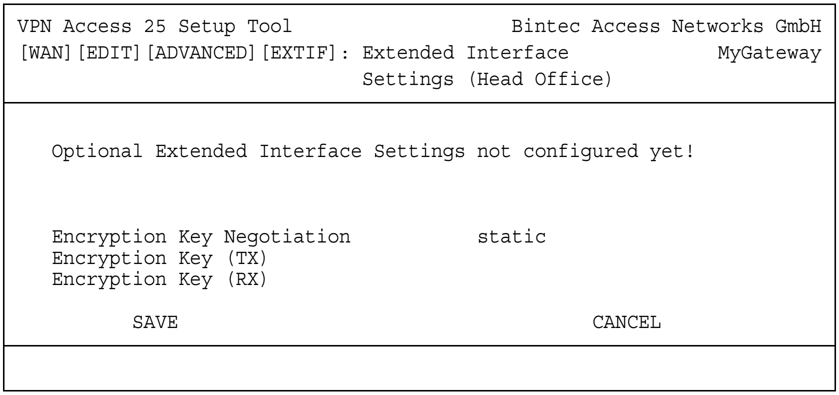
Field	**Description**
Callback	Enables a PPTP tunnel to be set up over the Internet to a PPTP partner, even if this partner is not online at the moment. The PPTP partner is usually requested by an ISDN call to go online and set up a PPTP connection. Possible values: ■ *yes (callback via PPTP VPN)*: Activates the callback function. ■ *no* (default value): Deactivates the callback function. Note that you must activate the relevant option on the gateways of both partners. An ISDN connection is usually required for this function. **VPN Access** series devices are equipped with various interfaces. Please refer to the data sheet or the **Technical Data** chapter of the manual to determine if your gateway is equipped with an ISDN interface. Without ISDN, callback is only to be activated in special applications.
Static Short Hold (sec)	The static short hold setting determines how many seconds should pass between sending the last ➤➤ traffic **data packet** and clearing the connection. Possible values are *-1* to *3600* (seconds). A value of *-1* means that the connection is set up again immediately after disconnection and *0* deactivates short hold. The default value is *20*.

Field	Description
Delay after Connection Failure (sec)	Indicates the wait time in seconds before the **VPN Access** gateway tries again after an attempt to establish a connection has failed (=block timer). The default value is *300*.
PPTP Mode	Here you enter the role of the PPTP interface. Possible values: ■ *PPTP PNS* (default value): PPTP network server; this assigns the PPTP interface the role of the PPTP server. ■ *Windows PPTP client mode*: This assigns the PPTP interface the role of the PPTP client.
Special Interface Types	This option permits special use of the interface. Possible values: ■ *none* (default value): No special type selected. ■ *dialin only*: Only incoming calls and callbacks initiated by the distant terminal are allowed for the interface. ■ *Call-by-Call (dialin only)*: The interface is defined as multi-user PPTP partner, which means several clients can log in with the same user name and password. Only practical for ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***BASIC IP SETTINGS*** ➜ ***IP ADDRESS NEGOTIATION*** = *dynamic server*.

Table 3-1: ***ADVANCED SETTINGS*** menu fields

3.1 Extended Interface Settings (optional) Submenu

The *Extended Interface Settings (optional)* submenu is described below.



```
VPN Access 25 Setup Tool                      Bintec Access Networks GmbH
[WAN][EDIT][ADVANCED][EXTIF]: Extended Interface              MyGateway
                              Settings (Head Office)


   Optional Extended Interface Settings not configured yet!



   Encryption Key Negotiation           static
   Encryption Key (TX)
   Encryption Key (RX)

          SAVE                                    CANCEL
```

The ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***Advanced Settings*** ➜ ***Extended Interface Settings*** submenu can be used to make additional settings for the ***Encryption Key Negotiation*** feature.

After saving the configuration for the first time in this menu, the message *Optional Extended Interface Settings not configured yet!* is grayed out and the **Delete Configuration** option is shown.

The ***Extended Interface Settings (optional)*** menu consists of the following fields:

Field	Description
Encryption Key Negotiation	Defines whether the key for any encryption enabled in ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***Encryption*** is generated automatically or defined statically. Possible values: ■ *authentication* (default value): Key is generated automatically by the **VPN Access** gateway. ■ *static*: The key is defined statically and must be entered under ***Encryption Key (TX)*** and ***Encryption Key (RX)***.
Encryption Key (TX)	(Only for ***Encryption Key Negotiation*** = *static*) Key in hexadecimal format for encryption of outgoing data (must be the same as the entry under ***Encryption Key (RX)*** at the connection partner).
Encryption Key (RX)	(Only for ***Encryption Key Negotiation*** = *static*) Key in hexadecimal format for encryption of incoming data (must be the same as the entry under ***Encryption Key (TX)*** at the connection partner).

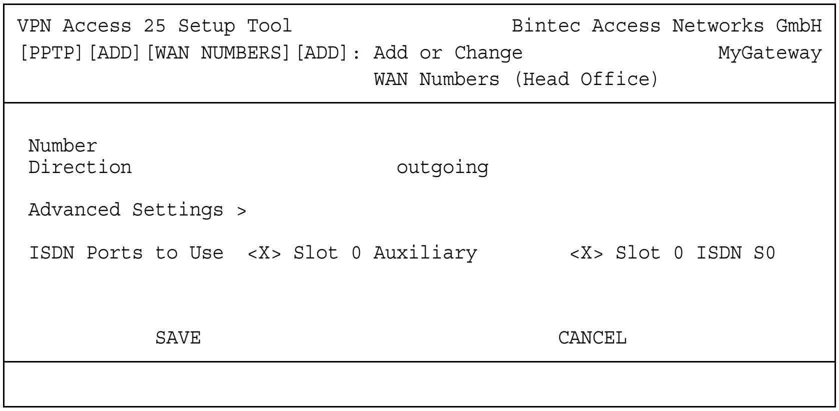
Table 3-2: ***Extended Interface Settings (optional)*** menu fields

4 WAN Numbers Submenu

The fields of the *WAN NUMBERS* submenu are described below.

The ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***WAN NUMBERS*** menu appears only if ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** is set to callback activated (see “Callback” on page 12).

Here the currently entered numbers of the PPTP partner are listed for the callback function. Other numbers can be added via the ***ADD*** button. Existing entries can be edited by selecting the relevant list entry.



```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][ADD][WAN NUMBERS][ADD]: Add or Change                  MyGateway
                               WAN Numbers (Head Office)

 Number
 Direction                       outgoing

 Advanced Settings >

 ISDN Ports to Use  <X> Slot 0 Auxiliary       <X> Slot 0 ISDN S0


            SAVE                               CANCEL
```

The ***WAN NUMBERS*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Number	Number of PPTP partner

Field	Description
Direction	Defines whether ***Number*** should be used for incoming or outgoing calls or for both. Possible values: - *outgoing* (default value): For outgoing initial calls to the PPTP partner for him to set up the PPTP tunnel. - *both (CLID)*: For incoming and outgoing calls. - *incoming (CLID):* For identification of an incoming initial call from the PPTP partner, so that the local gateway sets up a PPTP tunnel. The calling party number of the incoming call is compared with the number entered under ***Number***. The calling party number of a caller is also shown as ***Remote Number*** in ***Monitoring & Debugging*** ➜ ***ISDN Monitor***.

Field	Description
ISDN Ports to Use	Only for devices with ISDN S0 connection. Please refer to the data sheet for the **VPN Access** series at www.bintec.net to determine which interfaces are provided in your gateway. Defines the type of connection for callback: ■ Slot 0 Auxiliary ■ Slot 0 ISDN S0 *X* (default value) activates the respective entry and no entry deactivates the option. Note: If a modem is connected to the AUX interface of the gateway, activate only the type of connection desired for callback here. ISDN is selected here in the usual case. AUX should only be activated in special applications.

Table 4-1: ***WAN Numbers*** menu fields

Note

If your gateway is connected to a PABX for which a "0" trunk prefix is necessary for external line access, this "0" must be considered when entering the access number.

Wildcards

When entering the ***Number***, you can either enter the number digit for digit or you can replace single digits or groups of digits with wildcards. The ***Number*** can therefore be the same for various numbers.

The use of the wildcards shown in the following table has a different effect on incoming and outgoing calls:

Wildcard	Meaning		Example		
	Incoming calls	Outgoing calls	Number	The gateway accepts incoming calls, e.g. with:	Outgoing calls
*	Matches a group of none or more digits.	Is ignored.	123*	123, 1234, 123789	123
?	Matches exactly one digit.	Is replaced by 0.	123?	1234, 1238, 1231	1230
[a-b]	Defines a range of matching digits.	The first digit of the specified range is used.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Defines a range of prohibited digits.	The first digit after the specified range is used.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Optional sequence to match.	Sequence is used.	{00}1234	001234 and 1234	001234

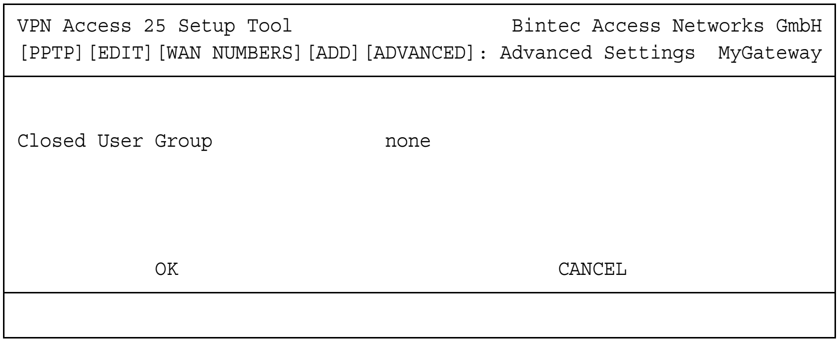
Table 4-2: Wildcards for incoming and outgoing calls

Note

If the calling party number of an incoming call matches both a PPTP partner's ***Number*** with wildcards and a PPTP partner's ***Number*** without wildcards, the entry without wildcards is always used.

4.1 Advanced Settings Submenu

The PPTP submenu ➜ ADD/EDIT ➜ WAN Numbers ➜ ADD/EDIT ➜ *Advanced Settings* is described below.



```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[PPTP][EDIT][WAN NUMBERS][ADD][ADVANCED]: Advanced Settings   MyGateway


Closed User Group                 none




             OK                                   CANCEL

```

The **VPN Access** gateway supports the use of the “Closed User Group” service feature, which you can request for your ISDN line from your telephone provider. The external/internal reachability is monitored and controlled by the exchanges if this feature is selected.

If no "Closed User Group" is defined, the ***Closed User Group*** (=CUG) field shows *none* (default value). To activate a Closer User Group, select *specify*. Enter the CUG index in the field that opens. You can obtain information about CUGs from your telephone provider.

5 IP Submenu

The *IP* submenu is described below.

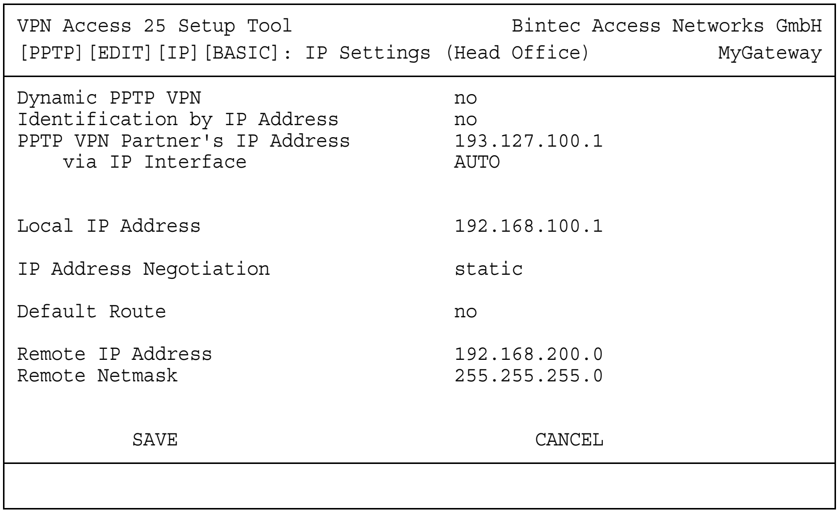
The ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** submenu is used for tasks such as making routing settings specifically for a PPTP partner.

The menu offers access to the submenus:

- ***BASIC IP SETTINGS***
- ***MORE ROUTING***
- ***ADVANCED SETTINGS.***

5.1 Basic IP Settings Submenu

The fields of the *BASIC IP SETTINGS* submenu are described below.



```
VPN Access 25 Setup Tool                        Bintec Access Networks GmbH
[PPTP][EDIT][IP][BASIC]: IP Settings (Head Office)                MyGateway

Dynamic PPTP VPN                      no
Identification by IP Address          no
PPTP VPN Partner's IP Address         193.127.100.1
    via IP Interface                  AUTO


Local IP Address                      192.168.100.1

IP Address Negotiation                static

Default Route                         no

Remote IP Address                     192.168.200.0
Remote Netmask                        255.255.255.0


          SAVE                               CANCEL
```

To be able to transfer IP packets between two PPTP tunnel endpoints, the gateway must know the route to the respective PPTP partner. In this menu you can define the basic route or generate a default route to the PPTP partner.

The ***Basic IP Settings*** menu consists of the following fields:

Field	Description
Dynamic PPTP VPN	Your gateway also supports PPTP tunnels to remote terminals with dynamic IP addresses. The respective PPTP partner must have a resolvable host name for this purpose, e.g. via a DynDNS provider. Possible values: ■ *yes*: Activates the feature. A DynDNS name can be entered in ***PPTP VPN Partner's IP Address***. ■ *no* (default value): Deactivates the feature. An IP address is entered in ***PPTP VPN Partner's IP Address***.
Identification by IP Address	Only for ***Dynamic PPTP VPN*** = *no*. ■ *yes*: The VPN partner is to be identified from his IP address. ■ *no* (default value)
PPTP VPN Partner's IP Address	The IP address of the PPTP partner. For a PPTP tunnel over the Internet, this must be a fixed official IP address. If you have selected *yes* for ***Dynamic PPTP VPN***, you must enter a resolvable host name here. If you still enter an IP address, ***Dynamic PPTP VPN*** is reset to *no* and the PPTP partner is searched for using the IP address entered.
via IP Interface	This field is shown if an IP address has been entered in ***PPTP VPN Partner's IP Address***. Here you select the IP interface over which packets are to be transported to the remote PPTP terminal. The default value is *AUTO*.

Field	Description
Use Gateway	This field is shown if an ETH interface is selected in ***VIA IP INTERFACE***. Defines whether the PPTP tunnel is implemented over a gateway. The default setting here is *no* and this should only be changed in special cases.
Gateway IP Address	Only if ***USE GATEWAY*** = *yes* IP address of the gateway connected.
Local PPTP VPN IP Address	This field is shown if an ETH interface is selected in ***VIA IP INTERFACE*** and ***USE GATEWAY*** = *no*. IP address of your gateway for the PPTP connection. This is an official IP address for a PPTP tunnel.
Local IP Address	Only if ***IP ADDRESS NEGOTIATION*** = *static.* Here you assign the PPTP interface an IP address from your LAN, which is used as the gateway's internal source address.
IP Address Negotiation	Here you select how the gateway's internal source address is determined. Possible values: ■ *static* (default value) - Fixed assignment of the IP address in ***LOCAL IP ADDRESS***. ■ *dynamic client* - Your gateway receives an IP address dynamically from the remote PPTP terminal. ■ *dynamic server* - The gateway assigns the remote PPTP terminal an IP address dynamically.

Field	Description
Enable NAT	Only if ***IP Address Negotiation*** = *dynamic client.* Defines whether Network Address Translation (=NAT) is activated for this connection. Possible values: ■ *yes*: NAT is activated. ■ *no* (default value): NAT is deactivated.
Default Route	Only if ***IP Address Negotiation*** = *static* or *dynamic client.* Defines whether the route to the PPTP partner is defined as default route. Possible values: ■ *yes*: The route to this PPTP partner is defined as default route. ■ *no* (default value): The route to this PPTP partner is not defined as default route.
Remote IP Address	Only if ***IP Address Negotiation*** = *static* and ***Default Route*** = *no.* Here you enter the IP address of the LAN of the PPTP partner.
Remote Netmask	Only if ***IP Address Negotiation*** = *static* and ***Default Route*** = *no.* Netmask of ***Remote IP Address***.

Table 5-1: ***Basic IP Settings*** menu fields

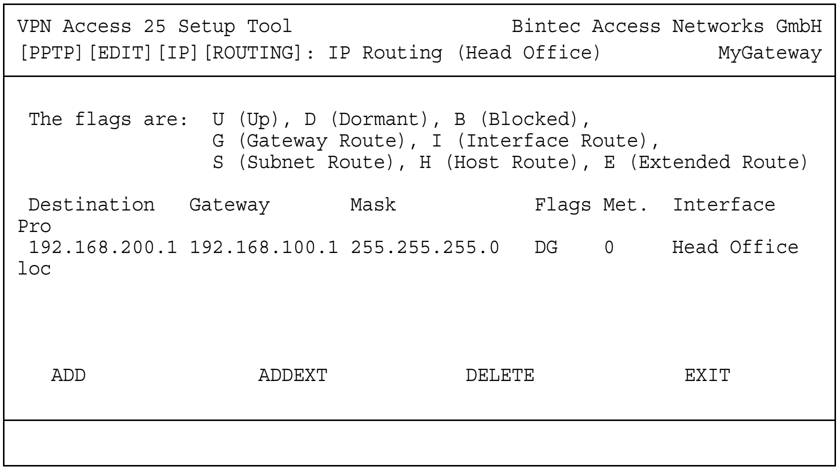
5.2 More Routing Submenu

The fields of the *More Routing* submenu are described below.

If a route has been entered for a specific PPTP partner in ***Basic IP Settings***, a routing entry is created automatically in your gateway's routing table. The ***More***

Routing submenu appears in the ***PPTP* ➜ *ADD/EDIT* ➜ *IP*** menu. In this menu you can edit the routing entries of a specific PPTP partner and add other entries.

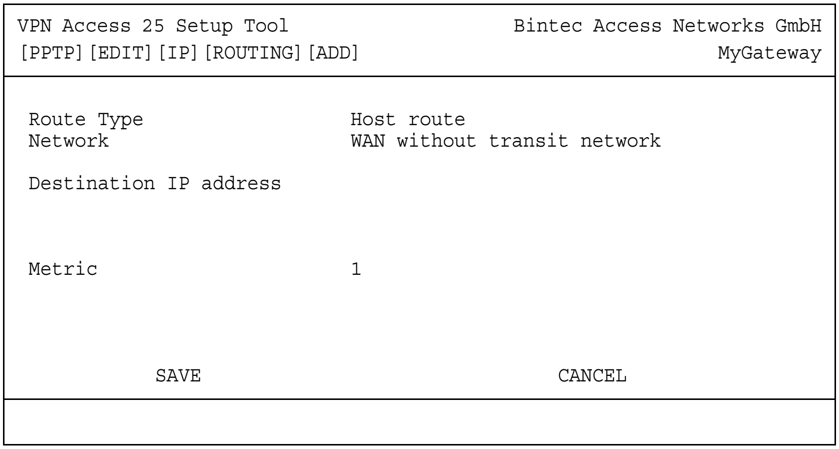
The IP routes of the specific PPTP partner are listed in the ***PPTP* ➜ *ADD/EDIT* ➜ *IP* ➜ *More Routing*** menu:



```
VPN Access 25 Setup Tool                     Bintec Access Networks GmbH
[PPTP][EDIT][IP][ROUTING]: IP Routing (Head Office)            MyGateway


 The flags are:  U (Up), D (Dormant), B (Blocked),
                 G (Gateway Route), I (Interface Route),
                 S (Subnet Route), H (Host Route), E (Extended Route)

 Destination   Gateway       Mask            Flags Met.  Interface
Pro
 192.168.200.1 192.168.100.1 255.255.255.0   DG    0     Head Office
loc



   ADD                ADDEXT             DELETE              EXIT
```

Flags shows the current status (*Up*, *Dormant*, *Blocked*) and the type of route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*). The protocol with which your gateway has "learned" the routing entry is displayed under ***Pro*** , e.g. *loc* = local, i.e. configured manually.

More routes are added in the ***PPTP* ➜ *ADD/EDIT* ➜ *IP* ➜ *More Routing* ➜ *ADD*** menu. Existing entries can be edited by tagging the desired list entry and pressing the Return key.



```
VPN Access 25 Setup Tool                      Bintec Access Networks GmbH
[PPTP][EDIT][IP][ROUTING][ADD]                                  MyGateway

 Route Type                    Host route
 Network                       WAN without transit network

 Destination IP address


 Metric                        1



            SAVE                                 CANCEL
```

The ***More Routing* ➜ *ADD/EDIT*** menu consists of the following fields:

Field	Description
Route Type	Type of route. Possible values: ■ *Host route* (default value): Route to a single host ■ *Network route*: Route to a network ■ *Default route*: The route is valid for all IP addresses and is only used if no other suitable route is available.
Network	Defines the type of connection. *WAN without transit network* is shown here for a PPTP partner. The value shown cannot be changed here.
Destination IP Address	Only if ***Route Type*** = *Host route* or *Network route*. IP address of the destination host or network.

Field	Description
Netmask	Only if ***ROUTE TYPE*** = *Network route*. Netmask for ***DESTINATION IP ADDRESS***. If no entry is made, the gateway uses a default netmask.
Metric	The lower the value, the higher the priority of the route (possible values *0*...*15*). The default value is *1*.

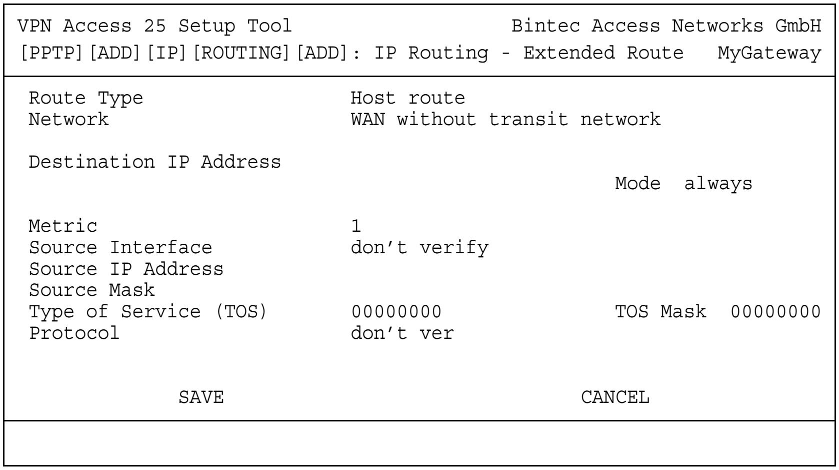
Table 5-2: ***MORE ROUTING*** menu fields

In addition to the normal routing table, the **VPN Access** gateway can also make routing decisions based on an Extended Routing Table. Apart from the source and destination address, the **VPN Access** gateway can also include the protocol, source and destination port, type of service (TOS) and the status of the destination interface in the decision.

Note

The entries in the Extended Routing Table are always treated preferentially over entries in the normal routing table.

Configuration is made in the ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***MORE ROUTING*** ➜ ***ADDEXT*** menu.



```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[PPTP][ADD][IP][ROUTING][ADD]: IP Routing - Extended Route   MyGateway

 Route Type                    Host route
 Network                       WAN without transit network

 Destination IP Address
                                                      Mode  always

 Metric                        1
 Source Interface              don't verify
 Source IP Address
 Source Mask
 Type of Service (TOS)         00000000               TOS Mask  00000000
 Protocol                      don't ver

              SAVE                                CANCEL
```

The menu contains the following fields:

Field	Description
Route Type	Type of route. Possible values: ■ *Host route* (default value): Route to a single host ■ *Network route*: Route to a network ■ *Default route*: The route is valid for all IP addresses and is only used if no other suitable route is available.
Network	Defines the type of connection. *WAN without transit network* is shown here for a PPTP partner. The value shown cannot be changed here.
Destination IP Address	Only if ***Route Type*** = *Host route* or *Network route* IP address of the destination host or network.
Netmask	Only if ***Route Type*** = *Network route* Netmask of ***Destination IP Address***.

Field	Description
Mode	Defines when the interface is to be used. For possible values see table "Mode selection options," on page 32.
Metric	The lower the value, the higher the priority of the route. Possible values *0...15*. Default value is *1*.
Source Interface	Interface over which the data packets reach the gateway. The default value is *don't verify*.
Source IP Address	IP address of the source host or network.
Source Mask	Netmask for ***SOURCE IP ADDRESS***.
Type of Service (TOS)	Possible values: *0..255* in binary format.
TOS Mask	Bit mask for ***TYPE OF SERVICE***.
Protocol	Defines a protocol. Possible values: *don't ver* (don't verify)*, icmp, ggp, tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp.* The default value is *don't ver*.
Source Port	Only if ***PROTOCOL*** = *tcp* or *udp* Source port number or range of source port numbers.
Destination Port	Only if ***PROTOCOL*** = *tcp* or *udp* Destination port number or range of destination port numbers.

Table 5-3: ***ADDEXT*** menu fields

MODE offers the following selection options:

Description	Meaning
always (default value)	Always use the route.

Description	Meaning
dialup wait	Use the route if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". Otherwise reroute.
dialup continue	Use the route if the interface is "up". If the interface is "dormant", then dial but reroute until the interface is "up". Otherwise reroute.
up only	Use the route if the interface is "up". Otherwise reroute.

Table 5-4: ***MODE*** selection options

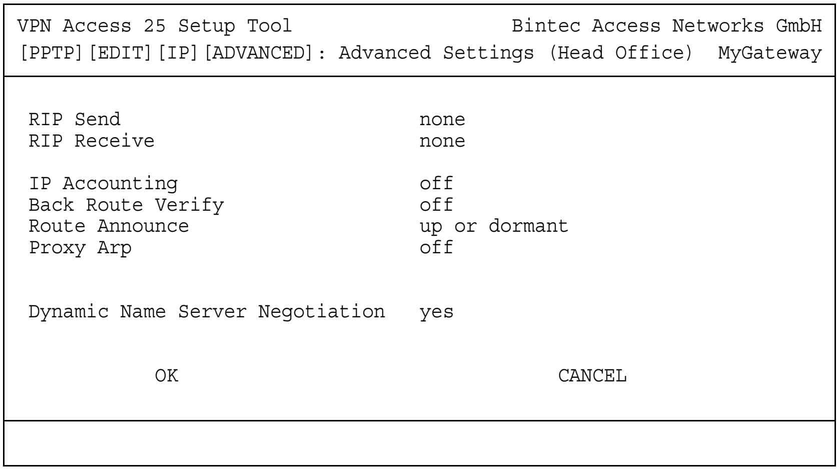
The ***SOURCE PORT*** and ***DESTINATION PORT*** fields contain the following selection options:

Description	Meaning
any (default value)	The route is valid for all ➤➤ **port** numbers.
specify	Enables the entry of a port number.
specify range	Enables the entry of a range of port numbers.
priv (0..1023)	Port numbers: 0 ... 1023
server (5000..32767)	Port numbers: 5000 ... 32767
clients 1 (1024..4999)	Port numbers: 1024 ... 4999
clients 2 (32768..65535)	Port numbers: 32768 ... 65535
unpriv (1024..65535)	Port numbers: 1024 ... 65535

Table 5-5: Selection options of ***SOURCE PORT*** and ***DESTINATION PORT***

5.3 Advanced Settings Submenu

The fields of the *ADVANCED SETTINGS* submenu are described below.



```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[PPTP][EDIT][IP][ADVANCED]: Advanced Settings (Head Office)   MyGateway

  RIP Send                               none
  RIP Receive                            none

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


  Dynamic Name Server Negotiation        yes


             OK                                      CANCEL
```

Extended routing settings for the respective PPTP partner can be made in the ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***ADVANCED SETTINGS*** menu.

RIP

The entries in the routing table can be defined statically or the routing table can be updated constantly by dynamic exchange of routing information between several gateways. This exchange is controlled by a Routing Protocol, e.g. RIP (Routing Information Protocol).

Gateways use the ➤➤ **RIP** to exchange information saved in their routing tables by communicating with each other at regular intervals. The **VPN Access** gateway supports both version 1 and version 2 of RIP, either individually or together.

RIP is configured separately for LAN and WAN.

Active and passive

Gateways can be defined as active or passive gateways: Active gateways offer their routing entries to other gateways via ➤➤ **broadcasts**. Passive gateways accept the information from the active gateways and store it, but do not pass on their own routing entries. The **VPN Access** gateway can be either active or passive.

PPTP partner

If you negotiate with a PPTP partner to receive and/or send RIP packets, your gateway can exchange routing information dynamically with the gateways in the LAN of the remote terminal.

Note

Receiving routing tables via the RIP is a possible security loophole, as external computers or gateways can change the routing functionality of the **VPN Access** gateway.

RIP packets do not set up or hold PPTP connections.

IP Accounting This option is for activating or deactivating the creation of IP accounting messages for this PPTP partner. If IP accounting is activated, a statistics message is generated (and entered in the **biboAdmSyslogTable**), which contains detailed information about the connections to this PPTP partner. (You will find settings for saving the accounting messages in a file in ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING***.)

Back Route Verify This term conceals a simple but very effective feature of the **VPN Access** gateway. If backroute verification is activated for an interface, incoming data packets are only accepted over this interface if outgoing answer packets are routed over the same interface. You can therefore prevent the acceptance of packets with fake IP addresses – even without filters.

Route Announce This option enables you to set when any activated routing protocols (e.g. RIP) are to propagate the IP routes defined for this interface.

Proxy Arp The ➤➤ **Proxy ARP** function enables the gateway to answer ➤➤ **ARP** requests from its own LAN on behalf of this specific PPTP partner. If a host in the LAN wants to set up a connection to another host in the LAN or to a PPTP partner but doesn't know its hardware address (MAC address), it sends a so-called ARP request into the network as a ➤➤ **broadcast**. If Proxy ARP is activated on the gateway and the desired destination host can be reached, for example, over a host route, the gateway answers the ARP request with its own hardware address. The ➤➤ **data packets** are sent to the gateway, which then forwards them to the desired host.

Note

Make sure that Proxy ARP is also activated on the LAN side.

The ***ADVANCED SETTINGS*** menu consists of the following fields:

Field	Description
RIP Send	Enables RIP packets to be sent over the interface to the PPTP partner. Possible values: see table “Selection options for RIP Send and RIP Receive,” on page 36.
RIP Receive	Enables RIP packets to be received over the interface to the PPTP partner. Possible values: see table “Selection options for RIP Send and RIP Receive,” on page 36.
IP Accounting	For creating accounting messages, e.g. for ➤➤ **TCP**, ➤➤ **UDP** and ICMP sessions. Possible values: *on*, *off* (default value).
Back Route Verify	Activates backroute verification for the interface to the PPTP partner. Possible values: *on, off* (default value).
Route Announce	Possible values: ■ *up or dormant* (default value): Routes are propagated if the interface status is *up* or *dormant*. ■ *always*: Routes are always propagated independent of operational status. ■ *up only*: Routes are only propagated if the interface status is *up*.
Proxy Arp	Enables the gateway to answer ARP requests from its own LAN on behalf of the specific PPTP partner. Possible values: see table “Proxy Arp selection options,” on page 37.

Field	Description
Dynamic Name Server Negotiation	Defines whether the **VPN Access** gateway receives IP addresses for ***Primary Domain Name Server, Secondary Domain Name Server, Primary WINS*** and ***Secondary WINS*** from the PPTP partner or sends them to the PPTP partner. For possible values see table "Dynamic Name Server Negotiation selection options," on page 38.

Table 5-6: ***Advanced Settings*** menu fields

RIP Send and ***RIP Receive*** contain the following selection options:

Description	Meaning
none (default value)	Not activated.
RIP V2 multicast	Only for ***RIP Send*** For sending RIP V2 messages over the multicast address 224.0.0.9.
RIP V1 triggered	RIP V1 messages are sent, received and processed as per RFC 2091 (triggered ➤➤ **RIP**).
RIP V2 triggered	RIP V2 messages are sent, received and processed as per RFC 2091 (triggered ➤➤ **RIP**).
RIP V1	For sending and receiving version 1 RIP packets.
RIP V2	For sending and receiving version 2 RIP packets.
RIP V1 + V2	For sending and receiving RIP packets of both version 1 and 2.

Table 5-7: Selection options for ***RIP Send*** and ***RIP Receive***

Proxy Arp offers the following selection options:

Description	Meaning
off (default value)	Deactivates Proxy ARP for this PPTP partner.
on (up or dormant)	The **VPN Access** gateway answers an ARP request only if the status of the connection to the PPTP partner is *up* (active) or *dormant* (idle). In the case of *dormant*, the **VPN Access** gateway only answers the ARP request; the connection is not set up until someone actually wants to use the route.
on (up only)	The **VPN Access** gateway answers an ARP request only if the status of the connection to the PPTP partner is *up* (active), i.e. a connection already exists to the PPTP partner.

Table 5-8: ***Proxy Arp*** selection options

Dynamic Name Server Negotiation contains the following selection options:

Description	Meaning
off	The **VPN Access** gateway sends or answers no requests for name server addresses.

Description	Meaning
yes (default value)	The meaning depends on the setting under ***IP ADDRESS NEGOTIATION*** in ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP***: ■ If *dynamic client* has been selected, the **VPN Access** gateway sends name server address requests to the PPTP partner. ■ If *dynamic server* has been selected, the **VPN Access** gateway answers name server address requests from the PPTP partner. ■ The **VPN Access** gateway answers, but sends no name server address requests if *yes* or *no* has been selected.
client (receive)	The **VPN Access** gateway sends name server address requests to the PPTP partner.
server (send)	The **VPN Access** gateway answers name server address requests from the PPTP partner.

Table 5-9: ***DYNAMIC NAME SERVER NEGOTIATION*** selection options

Index: PPTP