WAN PARTNER

Bintec User's Guide - VPN Access Series
Version 1.1

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 WAN Partner Menu

The fields of the *WAN PARTNER* menu are described below.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN]: WAN Partners                                          MyGateway

   Current WAN Partner Configuration

     Partnername                Protocol            State
     branch                     ppp                 dormant



   ADD                 DELETE              EXIT
```

To enable your gateway to set up connections to networks or hosts outside your LAN, you must configure the partners you want to connect to as so-called WAN partners on your gateway. This applies to outgoing connections (e.g. your gateway dials its WAN partner), as well as incoming connections (e.g. a WAN partner dials the number of your gateway) and leased lines.

If you want to access the Internet, you must set up your Internet Service Provider (➤➤ **ISP**) as a WAN partner. If you want to connect your LAN to a remote LAN, e.g. your LAN (head office) and the LAN of a branch office (corporate network connection), you must configure the remote LAN as a WAN partner.

If you have configured a leased line during configuration of your gateway's ISDN S0 interface, a WAN partner is already configured automatically in the ***WAN PARTNER*** menu. Edit this entry to suit your requirements.

All the WAN partners entered are displayed in a list that contains the partner name (***PARTNERNAME***), the encapsulation used (***PROTOCOL***) and the current state of each (***STATE***). ***PROTOCOL*** can have the possible values of ***ENCAPSULATION***, see table "Possible values for State field," on page 4.

The ***STATE*** field can have the following values:

Description	Meaning
up	connected
dormant	not connected (dialup connection); dial-up possible
blocked	not connected (e.g. an error occurred on setting up an outgoing connection, a renewed attempt is only possible after a specified number of seconds)
down	administratively set to *down* (deactivated); dial-up impossible for leased lines: not connected

Table 1-1: Possible values for ***STATE*** field

The WAN partner configuration is made in the ***WAN PARTNER*** ➜ ***ADD/EDIT*** menu:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][ADD]: Configure WAN Partner                              MyGateway

 Partner Name

 Encapsulation                  PPP
 Encryption                     none
 Compression                    none
 Calling Line Identification    no

 PPP >
 Advanced Settings >
 WAN Numbers >

 IP >
 Bridge >


              SAVE                          CANCEL
```

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

Field	Description
Partner Name	Enter a name for uniquely identifying the WAN partner. In this field the first character must not be a number. Don't use special characters or umlauts. The entry can have max. 25 characters.
Encapsulation	➤➤ **Encapsulation**. Defines how the ➤➤ **data packets** are packed for transfer to the WAN partner. Possible values: ■ *PPP* (default value) ■ *Multi-Protocol LAPB Framing* ■ *Multi-Protocol HDLC Framing* ■ *Async PPP over X.75* ■ *Async PPP over X.75/T.70/BTX* ■ *Async PPP over V.120 (HSCSD)* ■ *X.25_PPP* ■ *X.25* ■ *HDLC Framing (IP only)* ■ *LAPB Framing (IP only)* ■ *X31 B-Channel* ■ *X.25 No Signaling* ■ *X.25 PAD* ■ *X.25 No Configuration* ■ *Frame Relay*

Field	Description
Encapsulation (cont.)	■ *X.25 No Configuration, No Signaling* As not all Bintec devices support all protocols, please check prior to configuration the availablity of the respective protocol according to the data sheet at www.bintec.net.
Encryption	Defines the type of encryption that should be used for data traffic to the WAN partner. Only possible if STAC resp. MS-STAC compression is not activated for the connection. Possible values: see table “Encryption selection options,” on page 8. If ***ENCRYPTION*** is set, this function must also be activated at the remote gateway, otherwise the connection cannot be established.
Compression	Defines the type of compression that should be used for data traffic to the WAN partner and is only active when supported by the remote gateway. Possible values: ■ *STAC, MS-STAC, MPPC:* These values are only available if ***ENCAPSULATION*** has been set to *PPP*, *Async PPP* over *X.75*, *Async PPP* over *X.75*/*T.70*/*BTX*, *Async PPP* over *V.120 (HSCSD)* or *X.25_PPP*. ■ *V.42bis*: For ***ENCAPSULATION*** *LAPB Framing (only IP)* and *Multi-Protocol LAPB Framing* only V.42bis compression is available.

Field	Description
Compression (cont.)	■ *none* (default value) A combination of encryption and compression is only possible with (any) MPPE encryption and MPPC. When ***ENCAPSULATION*** = *Multi-Protocol HDLC Framing, X.25, HDLC Framing (only IP), X31 BChannel, X.25 No Signalling, X.25 PAD, X.25 No Configuration, Frame Relay* and *X.25 No Configuration, No Signalling* this field is not displayed. (As not all Bintec devices support all protocols, please check prior to configuration the availablity of the respective protocol according to the data sheet at www.bintec.net.)
Calling Line Identification	Indicates whether calls from this WAN partner are identified by means of the calling party number (➤➤ **CLID**). The value of this field depends on ***DIRECTION*** in the ***WAN NUMBERS*** submenu and cannot be set here.

Table 1-2: ***WAN PARTNER*** 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: required for MS clients as of Windows 2000 (MS service packs may be necessary, too)
MPPE V1 40 only	Only MPPE version 1 with 40-bit key

Description	Meaning
MPPE 56	MPPE version 1 and 2 with 56-bit key
MPPE V2 56	MPPE version 2 with 56-bit key
MPPE V2 56 (RFC 3078)	MPPE version 2 with 56-bit key as per RFC 3078: required for MS clients as of Windows 2000 (MS service packs may be necessary, too)
MPPE V1 56 only	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: required for MS clients as of Windows 2000 (MS service packs may be necessary, too)
MPPE V1 128 only	Only MPPE version 1 with 128-bit key
MPPE V1 128 (MS compatible mode)	MS compatible MPPE version 1 mode with 128-bit for MS-CHAP V1 (non-conform to RFC 3079)
MPPE V2 128 (MS compatible mode)	MS compatible MPPE version 2 mode with 128-bit for MS-CHAP V1 (non-conform to RFC 3079)
DES3 168	Triple DES with 168-bit key
Blowfish 168	Blowfish with 168-bit key

Table 1-3: ***ENCRYPTION*** selection options

These values are only available if ***ENCAPSULATION*** has been set to *PPP*, *Async PPP over X.75*, *Async PPP* over *X.75*/*T.70*/*BTX*, *Async PPP* over *V.120 (HSCSD)* or *X.25_PPP*. (As not all Bintec devices support all protocols, please

check prior to configuration the availablity of the respective protocol according to the data sheet at www.bintec.net.)

For all other possible values for ***ENCAPSULATION*** the field ***ENCRYPTION*** is not displayed.

1 WAN Partner Menu

2 Submenu PPP

The *PPP* submenu is described below.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][PPP]: PPP Settings (branch)                        MyGateway

  Authentication               CHAP + PAP
  Partner PPP ID
  Local PPP ID                 vpn25
  PPP Password

  Keepalives                   off
  Link Quality Monitoring      off


              OK                              CANCEL
```

The ***WAN PARTNER*** ➜ ***PPP*** menu contains specific ➤➤ **PPP** settings, e.g. ***AUTHENTICATION***, that only refer to the WAN partner to be configured. The gateway uses these settings to perform the authentication negotiation for outgoing calls, for incoming calls only if the WAN partner has been identified via CLID.

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

Field	Description
Authentication	Authentication protocol. Possible values: see table “Selection options in Authentication field,” on page 13.
Partner PPP ID	ID of WAN partner.
Local PPP ID	ID of your gateway. The set value of ***LOCAL PPP ID*** in the ***SYSTEM*** menu is default value.
PPP Password	Password.

Field	Description
Keepalives	Activates the function PPP-Keepalive for checking the reachability of the remote PPP terminal. Possible values: ■ *off* (default value for dialup connection) - deactivates keepalive. ■ *on* (default value for leased line) - activates keepalive. For the function PPP-Keepalive every three seconds a packet is sent to the remote terminal. If the packet is unanswered five times, normally the interface is set to *down* for leased line connections and *dormant* for dialup connections.
Link Quality Monitoring	Activates PPP Link Quality Monitoring as per RFC 1989. Possible values: ■ *off* (default value) ■ *on* Only necessary in exceptional cases, e.g. with Nokia Communicator.

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

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

Description	Meaning
PAP	Only run ➤➤ **PAP** (PPP Password Authentication Protocol); the password is transferred uncoded.
CHAP	Only run ➤➤ **CHAP** (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encoded.
CHAP + PAP	Run primarily CHAP, otherwise PAP.
MS-CHAP	Only run MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol).
CHAP + PAP + MS-CHAP	Run primarily CHAP, on denial 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

2 Submenu PPP

3 Submenu Advanced Settings

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][ADVANCED]: Advanced Settings (branch)              MyGateway

  Callback                                  no
  Static Short Hold (sec)                   20
  Idle for Dynamic Short Hold (%)           0
  Delay after Connection Failure (sec)      300
  Layer 1 Protocol                          ISDN 64 kbps

  Channel Bundling                          no


  Extended Interface Settings (optional) >


  Special Interface Types                   none

            OK                                        CANCEL
```

Specific functions for ➤➤ **WAN partners** make it possible to define the characteristics for connections to WAN partners individually and are configured in the ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS*** menu.

Callback

The callback mechanism can be used for each WAN partner to obtain additional security regarding the connection partner or to clearly allocate the costs of connections. A connection is not set up until the calling party has been clearly identified by calling back. The gateway can answer an incoming call with a callback or wait for a callback of a WAN partner.

Identification can be based on the calling party number or PAP/CHAP/MS-CHAP authentication. Identification is made in the first case without call acceptance, as the calling party number is transferred over the ISDN D-channel, and in the second case with call acceptance.

Defining short hold

➤➤ **Short hold** is defined to clear an unused connection automatically, i.e. when no more user data is sent, and thus save charges. The short hold setting

can be either static or dynamic and tells the gateway the duration of the idle time, after which it is to clear down the connection.

Static

The static short hold setting determines how much time should pass between sending the last ➤➤ user **data packet** and clearing the connection. Enter a fixed period of time in seconds.

Dynamic (only with ISDN)

With the dynamic short hold setting, no fixed period of time is specified and the length of an ISDN charging unit is considered instead. Dynamic short hold is based on AOCD (advice of charge during the call), which depends on time, weekend/weekday.

When setting dynamic short hold, you specify how much percent of an interval of charge may be reached after the last user data has been sent before the connection is cleared. If you enter 50 %, for example, the ***Idle for Dynamic Short Hold*** equals 60 seconds if the preceding charging unit was 120 seconds, and 300 seconds if the preceding charging unit was 600 seconds. Only use ***Idle for Dynamic Short Hold*** in conjunction with ***Static Short Hold*** for safety reasons.

Delay after connection failure

This function enables you to set the period of time the gateway is to wait for an attempt to set up an outgoing connection after an unsuccessful attempt to set up a call.

Layer 1 protocol

You can define the Layer 1 protocol for outgoing connections to the WAN partner.

Channel bundling

The gateway supports dynamic and static ➤➤ **channel bundling** for dialup connections. Only one B-channel is initially opened when a connection is established.

Dynamic

Dynamic channel bundling means that the gateway connects other ➤➤ **ISDN** B-channels to increase the throughput for connections to the WAN partner, if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional ➤➤ **B-channels** are closed again.

Static

In static channel bundling, you specify right from the start how many B-channels the gateway uses for connections to the WAN partner, regardless of the amount of data transferred.

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

Field	Description
Callback	Activates the callback function. Possible values: see table “Callback selection options,” on page 20.
Static Short Hold (sec)	Idle time in seconds for static short hold. Default value is *20*. e.g. *10* for FTP connections *20* for LAN to LAN connections *90* for Internet connections
Idle for Dynamic Short Hold (%)	Idle time in percent of the interval of charge for dynamic short hold. Only activate if charging pulses are transmitted during the connection (AOCD).
Delay after Connection Failure (sec)	Block timer. Indicates the wait time in seconds before the **VPN Access** gateway tries again after an attempt to establish a connection has failed.
Layer 1 Protocol	Defines which Layer 1 Protocol the **VPN Access** gateway is to use. This setting applies to outgoing connections with the WAN partner and to incoming calls from the WAN partner, only if they have been identified from the calling party number. Possible values: see table “Selection options of Layer 1 Protocol,” on page 21.

Field	Description
Channel Bundling	Defines whether and which type of channel bundling is to be used for ISDN connections to the WAN partner. Possible values: ■ *no:* No channel bundling, only one B-channel is ever available for connections. ■ *static:* Dynamic channel bundling. ■ *dynamic:* Static channel bundling. The field is not displayed when ***LAYER 1 PROTOCOL*** = *PPP over Ethernet (PPPoE)*, *PPP over PPTP*.
Total Number of Channels	For dynamic channel bundling: Defines the maximum number of B-channels that may be opened. For static channel bundling: Defines the number of B channels that are open throughout the connection.
Remote X.25 Address	X.25 destination address. Appears only if *AO/DI* is selected under ***LAYER 1 PROTOCOL***. As not all Bintec devices support all protocols, please check prior to configuration the availablity of the respective protocol according to the data sheet at www.bintec.net.

Field	Description
Special Interface Types	This option defines a special application of the interface. Possible values: ■ *none*: No special type selected. ■ *dialin only*: The interface is used for incoming dialup connections and for callback initiated from the outside. ■ *Call-by-Call (dialin only)*: The interface is defined as multi-user WAN partner, i.e. several clients dial in with the same user name and password. Only practical if ***WAN PARTNER*** ➜ ***IP*** ➜ ***BASIC SETTINGS*** ➜ ***IP TRANSIT NETWORK*** is set to *dynamic server.*

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

CALLBACK offers the following selection options:

Description	Meaning
no (default value)	The **VPN Access** gateway does not call back.
expected (awaiting callback)	The **VPN Access** gateway requests the WAN partner to call back.

Description	Meaning
yes (PPP negotiation)	The **VPN Access** gateway calls back after a period proposed by the Microsoft client (NT: 10 seconds, newer versions: 12 seconds) with the number with ***DIRECTION*** *outgoing* or *both* entered for the WAN partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided if possible for security reasons. However, for connecting mobile Microsoft ➤➤ **clients** over data transmission networks this is currently not avoidable.
yes (delayed, CLID only)	The **VPN Access** gateway calls back after approx. four seconds, if requested to by the WAN partner. Makes only sense with CLID.
yes (PPP negotiation, callback optional)	Like *yes (PPP negotiation)* with abort option. This option should be avoided for safety reasons. The Microsoft client additionally has the option of aborting callback and maintaining the initial connection to the **VPN Access** gateway without callback. This is only valid if no fix outgoing number has been configured for the WAN partner. This is done by pressing **CANCEL** to close the dialog box that appears.
yes	The **VPN Access** gateway calls back immediately, if requested to by the WAN partner.

Table 3-2: ***CALLBACK*** selection options

LAYER 1 PROTOCOL contains the following selection options. As not all Bintec devices support all protocols, please check prior to configuration the availablity of the respective protocol according to the data sheet at www.bintec.net.

Description	Meaning
ISDN 64 kbps (default value)	For 64-kbps ISDN data connections.
Modem	(Only available if expansion card and resource card with digital modems are installed) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource card that accepts this call uses the settings for Modem Profile 1, which were selected in the ***MODEM*** ➜ ***PROFILE CONFIGURATION*** ➜ ***PROFILE 1*** menu.
DOVB	Data transmission Over Voice Bearer – useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
V.110 (1200 ... 38400)	For GSM connections to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
Modem Profile 1 ... 8	(Only available if expansion card and resource card with digital modems are installed) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource card that accepts this call uses the settings for Modem Profile 1... 8, which were selected in the ***MODEM*** ➜ ***PROFILE CONFIGURATION*** ➜ ***PROFILE 1...8*** menu.
PPP over Ethernet (PPPoE)	For connections to xDSL
PPP over PPTP	For connections to xDSL, e.g. in Austria
AO/DI	For using Always On/Dynamic ISDN

Table 3-3: Selection options of ***LAYER 1 PROTOCOL***

3.1 Submenu Extended Interface Settings (optional)

The fields of the *EXTENDED INTERFACE SETTINGS* submenu are described below.

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

   Optional Extended Interface Settings not configured yet!


   Mode                                    Bandwidth On Demand Enabled
   Line Utilization Weighting              equal
   Line Utilization Sample (sec)           5
   Gear Up Threshold                       90
   Gear Down Threshold                     80

   Maximum Number of Dialup Channels       1

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

          SAVE                                          CANCEL
```

The ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS*** submenu displays per default only options for ***ENCRYPTION KEY NEGOTIATION***. If Channel Bundling is set to *dynamic*, further options for the function Bandwidth in Demand (=BOD) are shown. If BOD is activated in ***MODE***, additional options are displayed.

If you save the configuration of the options in this menu for the first time, the message *Optional Extended Interface Settings not configured yet!* is blanked out and the option ***DELETE CONFIGURATION*** is displayed.

Channel-Bundling

The Channel-Bundling function can only be applied with ISDN connections or leased lines in conjunction with ISDN for increasing bandwidth or as backup solution. The gateways of the **VPN Access** series are equipped with different

types of interfaces. See the user's guide part **Technical Data** or check the interfaces at the device to verify if your gateway has a BRI.

If the remote terminal uses a device of other makes, verify that dynamic channel bundling resp. BACP/BAP are supported also for leased lines in conjunction with ISDN for increase of bandwidth resp. as backup solution.

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

Field	Description
Mode	Only for ***WAN Partner*** ➜ ***Advanced Settings*** ➜ ***Channel-Bundling*** = *dynamic* Defines which mode is used for BOD. Possible values: see table "Mode selection options," on page 31.
Line Utilization Weighting	Only for ***Mode*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Defines how the line utilization is calculated. The load is calculated every 1 second. Possible values: ■ *equal*: All the measured values of throughput in ***Line Utilization Sample (sec)*** are weighted equally for the calculation (default value). ■ *proportional*: The last measured values of throughput are weighted more heavily for the calculation, i.e. in ***Line Utilization Sample (sec)*** the calculation is most heavily influenced by the last measured values.

Field	Description
Line Utilization Sample (sec)	Only for ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Time interval in seconds. Throughput measurements in ***LINE UTILIZATION SAMPLE (SEC)*** are included in the calculation of the line utilization (the load is calculated every 1 second). Possible values: *5* to *300* (default value: *5*).
Gear Up Threshold	Only for ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Utilization threshold in percent at which another ISDN B-channel is added for a connection.
Gear Down Threshold	Only for ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* A B-channel is dropped as soon as the remaining connection has a load measured in percent that is lower than the value adjusted in this field.

Field	Description
D-Channel Queue Length	(Only if ***LAYER 1 PROTOCOL*** = *AO/DI* in the ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS*** menu) See data sheet on www.bintec.net to check whether your gateway supports AO/DI. Only for ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Threshold value for the number of bytes accumulated in the buffer of the D-channel at which the system is to change to the B-Channel Mode. Default value is *7500*.
Maximum Number of Dialup Channels	Only for ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Maximum possible number of ISDN B-channels that can be opened for this WAN partner. The value is only displayed here; it is set under ***TOTAL NUMBER OF CHANNELS*** in the ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** menu. Default value is *1*.

Field	Description
Encryption Key Negotiation	Defines whether a key for the connection to the WAN partner is generated automatically or defined statically in case an encryption has been activated in ***WAN PARTNER*** ➜ ***ENCRYPTION***. 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 decryption of incoming data (must be the same as the entry under ***ENCRYPTION KEY (TX)*** at the connection partner).

Table 3-4: ***EXTENDED INTERFACE SETTINGS*** submenu fields

MODE offers the following selection options:

Description	Meaning
Bandwidth On Demand Disabled	Deactivates ➤➤ **BOD** (default value).

Description	Meaning
Bandwidth On Demand Enabled	(For dialup connections only) Activates BOD, additional ISDN B-channels can be opened. The connection partner who initiated the connection opens the additional channels.
BAP, Active Mode and *BAP, Passive Mode*	BAP=Bandwidth Allocation Protocol *BAP, Active Mode* must be set for ***LAYER 1 PROTOCOL*** = *AO/DI* (=Always On/Dynamic ISDN). The function AO/DI depends on the type of device. See data sheet on www.bintec.net to check whether your gateway supports it. The Bandwidth Allocation Protocol (BAP) has three different modes for negotiating a bandwidth change. The two negotiating partners take opposite roles. In this scenario the remote connection partner must always be in the opposite role or in *BAP, Active and Passive Mode*. The negotiating partners behave as follows: ■ Call Request: The partner in Active Mode wants to add a second B-channel. He sends a Call Request. A partner in Passive Mode accepts the Call Request of the negotiating partner if applicable. The partner in Active Mode thus opens the B-channel.

Description	Meaning
BAP, Active Mode and *BAP, Passive Mode* (cont.)	■ Callback Request: The partner in Active Mode requests the partner in Passive Mode to add a second B-channel. He sends a Callback Request. A partner in Passive Mode accepts the Callback Request if applicable and opens the channel. ■ Link Drop Request: The partner in Active Mode wants to drop a B-channel. He sends a Link Drop Request. A partner in Passive Mode accepts the Link Drop Request of the negotiating partner if applicable. The partner in Active Mode then drops the channel.
BAP, Active and Passive Mode	Choosing this option both negotiating partners can have the active or the passive role. The negotiating partners behave as follows: ■ Call Request: One of the two partners wants to add a second B-channel. He sends a Call Request, the partner accepts it. Both negotiating partners can send the Call Reqest as well as accept one. ■ Callback Request: One of the negotiating partners requests the other to add a second B-channel. He sends a Callback Request, the partner accepts it and opens the channel. Both partners can send a Callback Request as well as accept one. ■ Link Drop Request: One partner wants to drop a B-channel. He sends a Link Drop Request, the partner accepts it. Both partners can send a Link Drop Request as well as accept it.

Description	Meaning
BAP, Active and Passive Mode (cont.)	Ensure that at the remote gateway, *BAP, Client Active Mode* or with devices of other makes RFC 2125 is supported and a corresponding mode is activated.
BAP, Client Active Mode	BAP behaves as follows in Client Active Mode: The partner who initiated the call setup is in Active Mode (see ***BAP, ACTIVE MODE***) and the partner who accepted the call is in Passive Mode (see ***BAP, PASSIVE MODE***). Ensure that at the remote gateway, *BAP, Client Active Mode* or with devices of other makes RFC 2125 is supported and a corresponding mode is activated.
BAP, Dialup Client Mode and *BAP Dialup Server Mode*	(For dialup connections only) An ISP can fulfill the channel-bundling function, even if it distributes incoming calls to several gateways: an ISDN number is transmitted to the client who dials in. This number is assigned individually to each gateway on the central side, so that the calls on several channels to this number are always terminated on the same gateway. Adding the second B-channel is carried out via a kind of callback: the client requests a further B-channel. The central side then requests the individual number of the gateway to which the client has already been connected. In this scenario the client takes the active part, i.e. he controls and has the responsibility (costs for channel-bundling). The central side accepts all requests of the client as long as they match the WAN partner configuration on the gateway.

Description	Meaning
BAP, Dialup Client Mode and *BAP Dialup Server Mode* (cont.)	■ settings on client-side: *BAP, Dialup Client Mode* ■ settings on server-side: *BAP, dialup Server Mode* (additionally: configuration of further values as e.g. ***BAPNUMBER*** and ***BAPLKTYPE*** in the ***PPPDIALPROFILETABLE*** via the SNMP shell of your gateway) Channel-Bundling must be activated on both sides (see ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***CHANNEL BUNDLING*** set to *dynamic* or *static*). If dial-in authentication is carried out via a RADIUS-Server, the Bintec-specific attributes must be applied for the configuration of the RADIUS-Server. Therefore an entry must be written into the user's file, that generates the required entries into the ***PPPEXTIFTABLE***.
Backup	(For leased lines only) The backup connection is activated if the leased line fails. The backup connection is cleared when the leased line is available again. BOD is also available for this mode, if a value > *1* is used for ***MAXIMUM NUMBER OF DIALUP CHANNELS***. One additional BRI for dial-up connections must be available at least. See datasheet on www.bintec.net to check with how many BRIs your gateway is equipped.

Description	Meaning
Bandwidth On Demand Active and *Bandwidth On Demand Passive*	(For leased lines only) Enables BOD. *Bandwidth On Demand Active* defines the active partner. This side activates adding and dropping additional B-channels on demand. *Bandwidth On Demand Passive* defines the passive partner.

Table 3-5: ***MODE*** selection options

4 Submenu WAN Numbers

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

The ***WAN PARTNER*** ➜ ***WAN NUMBERS*** menu contains a list of the numbers entered for the WAN partner. 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
[WAN][EDIT][WAN NUMBERS][ADD]: Add or Change                  MyGateway
                               WAN Numbers (branch)

 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 WAN partner.

Field	Description
Direction	Defines whether ***NUMBER*** should be used for incoming or outgoing calls or for both. Possible values: ■ *outgoing*: For outgoing calls, where you dial your WAN partner. ■ *both (CLID)*: For incoming and outgoing calls. ■ *incoming (CLID):* For incoming calls, where your WAN partner dials in to your gateway. The Calling Party Number of the incoming call is compared with the set ***NUMBER***. The Calling Party Number can be read in ***MONITORING & DEBUGGING*** ➜ ***ISDN MONITOR*** as ***REMOTE NUMBER***.
ISDN Ports to Use	(Only for devices with ISDN S0 interface. See datasheet for **VPN Access** series at www.bintec.net for available interfaces.) Defines the ISDN ports to be used. ■ Slot 0 Auxiliary: no entry or *X* ■ Slot 0 ISDN S0: no entry or *X*

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

Note When the gateway is connected to a PABX system for which a "0" 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 extension digit for digit or you can replace single numbers or groups of numbers with wildcards. ***NUMBER*** can therefore equal various extensions.

You can use the following wildcards, which have different effects for incoming and outgoing calls:

Wildcard	Meaning		Example		
	Incoming calls	Outgoing calls	Number	The gateway accepts incoming calls e.g. with:	Outgoing calls, i.e. the gateway sets up a connection to the WAN partner with:
*	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 excluded 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 WAN partner's ***NUMBER*** with wildcards and a WAN partner's ***NUMBER*** without wildcards, the entry without wildcards is always used.

4.1 Submenu Advanced Settings

The *WAN NUMBERS* ➜ *ADVANCED SETTINGS* submenu is described below.

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 company. The reachability of your ISDN S0 interface 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*. To activate a Closer User Group for a WAN partner, select *specify*. Enter the CUG index in the field that opens. You can obtain information about CUGs from your telephone provider.

5 Submenu IP

The *IP* submenu is described below.

The ***WAN PARTNER*** ➜ ***IP*** submenu is used for making routing settings specifically for a WAN partner.

The ***IP*** submenu consists of the following additional submenus:

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

5.1 Submenu Basic IP-Settings

The fields of the *BASIC IP-SETTINGS* submenu are described below. When *TRANSIT NETWORK* is set to *yes*, the following screen is displayed (example addresses are used here):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][IP][BASIC]: IP Settings (branch)                  MyGateway


 IP Transit Network                    yes



 Local IP Address                      192.168.100.1
 Partner IP Address                    192.168.100.2


 Default Route                         no

 Remote IP Address                     192.168.1.0
 Remote Netmask                        255.255.255.0


          SAVE                                CANCEL
```

To be able to transfer IP datagrams between two remote LANs, the gateway must know the route to the respective destination network. In this menu you can define the basic routing or generate a default route to the partner gateway.

Default route All data is sent automatically to the WAN partner on a default route, if no other route matches.

Setting up an Internet connection, you should configure the route to your Internet Service Provider (ISP) as a default route.

If you configure e.g. a corporate network connection, only enter the route to the head office as a default route if you do not configure Internet access over your gateway.

If you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office.

You can configure several default routes on your gateway, but only one can be active. Make sure that you set different values for ***METRIC***, if you configure more than one default route.

Transit network You use an additional ISDN IP address each for your gateway and the WAN partner. This sets up a virtual IP network – called a transit network – during the connection. You do not normally need this setting, but it is necessary for some special configurations.

If in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***LAYER 1 PROTOCOL*** other options than *PPP over PPTP* are set, the ***BASIC IP-SETTINGS*** menu consists of the following fields:

Field	Description
IP Transit Network	Defines whether your gateway uses a transit network to the WAN partner. Possible values: ■ *yes*: The transit network is used. ■ *no* (default value): The transit network is not used. ■ *dynamic client*: Your gateway receives an IP address dynamically. ■ *dynamic server*: Your gateway assigns IP addresses to the remote gateway dynamically.
Local IP Address	Only for ***IP TRANSIT NETWORK*** = *yes, no*. ■ if *yes* = WAN IP address of your gateway ■ if *no* = LAN IP address of your gateway
Partner IP Address	Only if *yes* is set for ***IP TRANSIT NETWORK***. WAN partner's WAN IP address in the transit network.
Enable NAT	Only if *dynamic client* is set for ***IP TRANSIT NETWORK***. Possible values: ■ *yes*: NAT is activated for this WAN partner. ■ *no* (default value): NAT is deactivated for this WAN partner. The settings in this menu correspond to NAT activation in the ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT*** menu.

Field	Description
Default Route	Only if *dynamic client, no* or *yes* is set for ***IP TRANSIT NETWORK***. Possible values: ■ *yes*: Route to this WAN partner is defined as default route. ■ *no* (default value): Route to this WAN partner is not defined as default route.
Remote IP Address	Only if *yes* or *no* is set for ***IP TRANSIT NETWORK***. WAN partner's LAN IP address.
Remote Netmask	Only if *yes* or *no* is set for ***IP TRANSIT NETWORK***. WAN partner's LAN netmask.

Table 5-1: ***BASIC IP SETTINGS*** menu fields

For an xDSL connection via PPTP, e.g. by Telekom Austria, *PPP over PPTP* is set in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***LAYER 1 PROTOCOL***. Then the ***BASIC IP-SETTINGS*** menu consists of the following fields:

Field	Description
PPTP VPN Partner's IP Address	Here you enter the IP address of the PPTP remote terminal of your Internet Service Provider (=ISP).
via IP Interface	This field is displayed if an IP address has been entered into the field ***PPTP VPN PARTNER'S IP ADDRESS***. Here you select the IP interface via which packets from/to the PPTP remote terminal are transported.
Use Gateway	This field is displayed, when an interface has been selected in ***VIA IP INTERFACE***. Defines whether the PPTP tunnel is carried out via another gateway. Default value is *no*, which should only be modified in special applications.

Field	Description
Gateway IP Address	Only if ***USE GATEWAY*** = *yes* IP address of the gateway activated by setting ***USE GATEWAY*** to *yes*.
Local PPTP VPN IP Address	This field is displayed, if an interface has been selected in ***VIA IP INTERFACE*** and if ***USE GATEWAY*** is set to *no*. IP address of your gateway for the PPTP connection.
Enable NAT	Defines if Network Address Translation is active. Possible values: ■ *yes*: NAT is activated for this WAN partner. ■ *no* (default value): NAT is deactivated for this WAN partner.
Default Route	Defines if the route to this WAN partner is set as default route. Possible values: ■ *yes*: Route to this WAN partner is defined as default route. ■ *no* (default value): Route to this WAN partner is not defined as default route.

5.2 Submenu More Routing

The fields of the *MORE ROUTING* submenu are described below.

If a route has been entered for a specific WAN partner in ***BASIC IP-SETTINGS***, a routing entry is created automatically in your gateway's routing table. The submenu ***MORE ROUTING*** appears in the ***WAN PARTNER*** ➜ ***IP*** menu. In this menu you can edit the routing entries of a specific WAN partner and add other entries.

All the IP routes entered are listed in the ***IP*** ➜ ***MORE ROUTING*** menu:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][ADD][IP][ROUTING]: IP Routing (branch)                  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
 192.168.1.0   192.168.100.2  255.255.255.0  DG    1     branch      loc
 192.168.100.2 192.168.100.1  255.255.255.0  DH    1     branch      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***.

More routes are added in the ***WAN PARTNER*** ➜ ***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
[WAN][EDIT][IP][ROUTING][EDIT]                                MyGateway

 Route Type                  Network route
 Network                     WAN with transit network

 Destination IP Address      192.168.1.0
 Netmask                     255.255.255.0

 Gateway IP-Address          192.168.100.2
 Metric                      0


           SAVE                                  CANCEL
```

The ***MORE ROUTING*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Field	Description
Route Type	Type of route. Possible values: ■ *Host route*: Route to a single host ■ *Network route*: Route to a network ■ *Default route*: Is only used if no other suitable route is available.
Network	Defines the type of connection. For possible values see table “Selection options in Network field,” on page 44. The displayed value cannot be modified in this menu. It depends on the setting of ***IP TRANSIT NETWORK IN WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***BASIC IP-SETTINGS.***
Destination IP Address	Only for ***ROUTE TYPE*** *Host route* or *Network route*. IP address of the destination host or LAN.

Field	Description
Netmask	Netmask of the partner LAN (only possible for ***ROUTE TYPE*** = *Network route*; if no entry is made the gateway uses a standard netmask).
Gateway IP Address	Only for ***NETWORK*** *WAN with transit network*. IP address of the host to which your gateway should forward the IP packets.
Metric	The lower the value, the higher the priority of the route (possible values *0...15*).

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

NETWORK offers the following selection options:

Description	Meaning
WAN without transit network	Route to a destination host or LAN that can be reached via a WAN partner without including any transit network available.
WAN with transit network	Route to a destination host or LAN that can be reached via a WAN partner via a transit network.

Table 5-3: Selection options in ***NETWORK*** field

In addition to the normal routing table, the **VPN Access** gateway can also make routing decisions based on an additional table called the Extended Routing Table (Extended IP Routing). 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. If there are entries in the Extended Routing Table, these are treated preferentially compared with entries in the normal routing table.

To create extended IP routing entries, press the ***ADDEXT*** button to open the relevant menu.

Example Extended IP Routing (XIPR) is useful, for example, if two networks are connected via ISDN with a LAN-LAN connection, but certain services (e.g. Telnet)

should be routed over an X.25 link and not over an ISDN switched connection. By making entries in the Extended Routing Table, you can allow part of the IP traffic to run over the ISDN switched connection and part of the IP traffic (e.g. for Telnet) to run over an X.25 link.

Configuration is made in the Setup Tool menu ***WAN PARTNER ➜ IP ➜ MORE ROUTING ➜ ADDEXT***.

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

 Route Type                 Host route
 Network                    WAN without transit network

 Destination IP Address


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


             SAVE                                  CANCEL
```

The menu contains the following fields:

Field	Description
Route Type	Type of route. Possible values: ■ *Host route*: Route to a single host ■ *Network route*: Route to a network ■ *Default route*: Is only used if no other suitable route is available.

Field	Description
Network	Defines the type of connection, see table “Selection options in Network field,” on page 44. The displayed value cannot be modified in this menu. It depends on the setting of ***IP Transit Network in WAN Partner*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***Basic IP-Settings.***
Destination IP Address	Only for ***Route Type*** = *Host route* or *Network route* IP address of the destination host or LAN.
Netmask	Only for ***Route Type*** = *Network route* Netmask of ***Destination IP-Address***.
Partner / Interface	Displays the WAN partner (only possible for ***Network*** = *WAN without transit network*). Field cannot be modified.
Mode	Only for ***Network*** = *WAN without transit network*. Defines when the WAN partner is to be used. Possible values see table “Mode selection options,” on page 47
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. Default value is *don’t verify*.
Source IP-Address	Source IP address of the source host or LAN.
Source Mask	Netmask of ***Source IP-Address***.
Type of Service (TOS)	Possible values: *0..255* as bit string.
TOS Mask	Bit mask for ***Type of Service***.

Field	Description
Protocol	Defines a protocol. Possible values: *don't verify, icmp, ggp, tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp.* Default value is *don't verify*.
Source Port	Only for ***PROTOCOL*** = *tcp, udp* Source port number or range of source port numbers.
Destination Port	Destination port number or range of destination port numbers. Only for ***PROTOCOL*** = *tcp, udp*

Table 5-4: ***ADDEXT*** menu fields

The ***MODE*** field includes the following selection options:

Description	Meaning
always	Always use the route.
dialup wait	Use the route if the interface is "*up*". If the interface is "*dormant*", 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*", dial but reroute until the interface is "*up*". Otherwise reroute.
up only	Use the route if the interface is "*up*". Otherwise reroute.

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

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

Description	Meaning
any	All ➤➤ **port** numbers match the route.
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 5-6: Selection options of ***SOURCE PORT*** and ***DESTINATION PORT***

5.3 Submenu Advanced Settings

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

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


RIP Send                                 none
RIP Receive                              none

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

Van Jacobson Header Compression          off
Dynamic Name Server Negotiation          yes


              OK                                        CANCEL
```

Extended routing settings and other adjustments for the respective WAN partner can be made in the ***WAN Partner*** ➜ ***IP*** ➜ ***Advanced Settings*** menu.

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

Gateways use ➤➤ **RIP** to exchange information stored in routing tables by communicating with each other at regular intervals to mutually supplement and replace their routing entries. 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.

WAN partner

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

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 dialup connections.

IP Accounting This option is for activating or deactivating the creation of IP accounting messages for this WAN 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 WAN partner. (Settings for storage of accounting messages into a file can be done in ***System*** ➜ ***External System Logging***.)

Back Route Verification This term conceals a simple but very powerful function of the **VPN Access** gateway. If Backroute Verification is activated for a WAN partner, data packets are only accepted at the interface if answering packets would be routed over the same interface. You can therefore prevent packets with fake IP addresses being accepted – even without filters.

Route Announce This option enables you to set when routing protocols (e.g. RIP), that have been activated if applicable, propagate the IP routes defined for this interface.

Proxy ARP ➤➤ **Proxy ARP** enables the gateway to answer ➤➤ **ARP** requests from its own LAN acting for the defined WAN partner. If a host in the LAN wants to set up a connection to another host in the LAN or to a WAN partner, but doesn't know its hardware address (MAC address), it sends an ARP request as a ➤➤ **broadcast** to the network. If Proxy ARP is activated on the gateway and the desired target host can be reached e.g. via a host route, the gateway answers the ARP request with its own hardware address. This is sufficient for establishing the connection: The ➤➤ **data packets** are sent to the gateway, which then forwards them to the desired host.

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

Field	Description
RIP Send	Enables RIP packets to be sent via the interface to the WAN partner. Possible values: see table “Selection options for RIP Send and RIP Receive,” on page 53.
RIP Receive	For receiving RIP packets via the interface to the WAN partner. Possible values: see table “Selection options for RIP Send and RIP Receive,” on page 53.
IP Accounting	For generating accounting messages for e.g. ➤➤ **TCP**, ➤➤ **UDP** and ICMP sessions. Possible values: *on*, *off* (default value).
Back Route Verify	Activates Back Route Verification for the interface to the WAN partner. Possible values: *on, off* (default value).
Route Announce	Possible values: ■ *up or dormant* (default value): Routes are propagated if the interface’s 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 **VPN Access** gateway to answer ARP requests from the own LAN acting for the defined WAN partner. Possible values: see table “Proxy ARP selection options,” on page 53.

Field	Description
Van Jacobson Header Compression	Reduces the size of the TCP/IP packet. Possible values: ■ *on*: VJHC activated. ■ *off*: VJHC deactivated.
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 WAN partner or sends them to the WAN partner. For possible values see table "Dynamic Name Server Negotiation selection options," on page 54.

Table 5-7: ***ADVANCED SETTINGS*** menu fields

RIP SEND and ***RIP RECEIVE*** contain the following selection options:

Description	Meaning
none	Not activated.
RIP V2 multicast	Only for ***RIP SEND*** The gateway waits for version 2 RIP packets with RIP V2 multicast address 224.0.0.9.
RIP V1 triggered	RIP V1 messages are sent rsp. received and processed as per RFC 2091 (Triggered ➤➤ **RIP**).
RIP V2 triggered	RIP V2 messages are sent rsp. 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.

Description	Meaning
RIP V1 + V2	For sending and receiving RIP packets of both version 1 and 2.

Table 5-8: Selection options for ***RIP SEND*** and ***RIP RECEIVE***

PROXY ARP offers the following selection options:

Description	Meaning
off	Deactivates Proxy ARP for this WAN partner.
on (up or dormant)	The **VPN Access** gateway answers an ARP request only if the status of the connection to the WAN 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 WAN partner is *up* (active), i.e. a connection already exists to the WAN partner.

Table 5-9: ***PROXY ARP*** selection options

DYNAMIC NAME SERVER NEGOTIATION contains the following selection options:

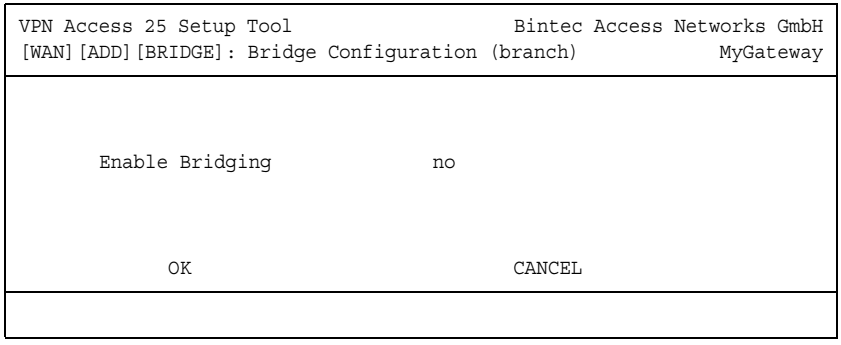
Description	Meaning
off	The **VPN Access** gateway sends or answers no requests for name server addresses.

Description	Meaning
yes	The meaning depends on the settings in ***WAN PARTNER*** ➜ ***EDIT*** ➜ ***IP*** under ***IP TRANSIT NETWORK***): ■ If *dynamic client* has been selected, the **VPN Access** gateway sends Name Server Address Requests to the WAN partner. ■ If *dynamic server* has been selected, the **VPN Access** gateway answers Name Server Address Requests from the WAN partner. ■ If *yes* or *no* has been selected, the **VPN Access** gateway answers, but sends no Name Server Address Requests .
client (receive)	The **VPN Access** gateway sends Name Server Address Requests to the WAN partner.
server (send)	The **VPN Access** gateway answers Name Server Address Requests from the WAN partner.

Table 5-10: ***DYNAMIC NAME SERVER NEGOTIATION*** selection options

6 Submenu Bridge

The *BRIDGE* submenu is described below.



The **VPN Access** gateway can be operated in Bridging Mode.

In contrast to a ➤➤ **router**, bridges operate at layer 2 of the ➤➤ **OSI model**, are independent of higher-level protocols and transmit data packets using ➤➤ **MAC addresses**.

Bridges are used to physically decouple networks and to reduce network data traffic. This is done by using filter functions that allow data packets to pass to certain network segments only.

To operate the **VPN Access** gateway in Bridging Mode, the function must be activated in the field ***BRIDGING*** for the respective Ethernet interface of the LAN.

To include the defined WAN partner in the bridging function, the value in the ***ENABLE BRIDGING*** field is set to *yes* (default value is *no*).

6 Submenu Bridge

Index: WAN Partner