WAN PARTNER

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von BinTec Gateways ab Software-Release 7.1.1. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind immer zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Bintec Access Networks GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Bintec Access Networks GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Bintec Access Networks GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Bintec erreichen

Bintec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.bintec.de

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 Hauptmenü

Im folgenden werden die Felder des Menüs *WAN PARTNER* beschrieben.

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

   Current WAN Partner Configuration

     Partnername                Protocol            State



   ADD                 DELETE              EXIT
```

Um mit Ihrem Gateway Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als WAN Partner auf Ihrem Gateway einrichten. Dies gilt sowohl für ausgehende Verbindungen (Ihr Gateway wählt sich bei einem WAN Partner ein), als auch für eingehende Verbindungen (ein WAN Partner wählt sich bei Ihrem Gateway ein) und Festverbindungen.

Wenn Sie z. B. einen Internetzugang herstellen wollen, müssen Sie Ihren Internet-Service-Provider (➤➤ **ISP**) als WAN Partner einrichten. Wenn Sie eine LAN-LAN-Kopplung aufbauen wollen, z. B. zwischen Ihrem LAN (Firmenzentrale) und dem LAN einer Filiale (Firmennetzanbindung), müssen Sie das LAN der Filiale als WAN Partner einrichten.

Wenn Sie bei der Konfiguration der WAN-Schnittstelle(n) Ihres Gateways eine oder mehrere Festverbindungen (z. B. PPTP-Verbindungen) eingerichtet haben, wird im Menü ***WAN PARTNER*** bereits automatisch jeweils ein WAN Partner angelegt. Editieren Sie diesen Eintrag entsprechend Ihren Erfordernissen.

Alle eingetragenen WAN Partner werden in einer Liste angezeigt, die den Partnernamen (***PARTNERNAME***), die verwendete Enkapsulierung (***PROTOCOL***) und den aktuellen Status (***STATE***) enthält.

Das Feld ***STATE*** kann folgende mögliche Werte annehmen:

Wert	Bedeutung
up	verbunden.
dormant	nicht verbunden (Wählverbindung).
blocked	nicht verbunden (aufgrund eines Fehlers beim Verbindungsaufbau ist ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich).
down	administrativ auf *down* gesetzt (deaktiviert); bei Festverbindungen: nicht verbunden.

Tabelle 1-1: Mögliche Werte im Feld ***STATE***

Die Konfiguration der WAN Partner erfolgt im Menü ***WAN PARTNER*** ➜ ***ADD/EDIT***:

```
VPN Access 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 >
 Weekly Schedule >

 IP >
 Bridge >


              SAVE                              CANCEL
```

Das Menü ***WAN PARTNER*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Partner Name	Geben Sie einen beliebigen Namen ein, um den WAN Partner eindeutig zu benennen.
Encapsulation	➤➤ **Enkapsulierung**. Definiert, wie die ➤➤ **Datenpakete** für die Übertragung zum WAN Partner verpackt werden. Mögliche Werte: ■ *PPP* (Defaultwert) ■ *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 (only IP)* ■ *LAPB Framing (only IP)* ■ *X31 B-Channel* ■ *X.25 No Signalling* ■ *X.25 PAD* ■ *X.25 No Configuration* ■ *Frame Relay* ■ *X.25 No Configuration, No Signalling*

Feld	Wert
Encryption	Definiert die Art der Verschlüsselung, die für den Datenverkehr mit dem WAN Partner angewendet werden soll. Nur möglich, wenn keine Komprimierung mit STAC für die Verbindung aktiviert ist. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Encryption” auf Seite 7
Compression	Legt die Art der Komprimierung fest, die für den Datenverkehr mit dem WAN Partner angewendet werden soll. Mögliche Werte: ■ *STAC* ■ *MS-STAC* ■ *MPPC* ■ *none* Diese Werte sind nur verfügbar, wenn unter ***ENCAPSULATION*** *PPP*, *Async PPP* over *X.75*, *Async PPP* over *X.75/T.70/BTX*, *Async PPP* over *V.120 (HSCSD)* oder *X.25_PPP* ausgewählt wurde. Für ***ENCAPSULATION*** *LAPB Framing (only IP)* und *Multi-Protocol LAPB Framing* steht V.42bis-Komprimierung zur Verfügung. Eine Kombination von Verschlüsselung und Kompression ist nur mit einer (beliebigen) MPPE-Verschlüsselung und MPPC möglich.
Calling Line Identification	Zeigt an, ob Rufe von diesem WAN Partner anhand der "Calling Party Number" identifiziert werden sollen (➤➤ **CLID**). Der Wert des Feldes ist abhängig von ***DIRECTION*** im Untermenü ***WAN NUMBERS*** und kann hier nicht gesetzt werden.

Tabelle 1-2: Felder im Menü ***WAN PARTNER***

ENCRYPTION enthält folgende Auswahlmöglichkeiten:

Feld	Wert
MPPE 40	MPPE Version 1 mit 40-Bit-Schlüssel
MPPE 56	MPPE Version 1 mit 56-Bit-Schlüssel
MPPE 128	MPPE Version 1 mit 128-Bit-Schlüssel
MPPE V2 40	MPPE Version 2 mit 40-Bit-Schlüssel
MPPE V2 56	MPPE Version 2 mit 56-Bit-Schlüssel
MPPE V2 128	MPPE Version 2 mit 128-Bit-Schlüssel
MPPE V2 40 (RFC 3078)	MPPE Version 2 mit 40-Bit-Schlüssel gemäß RFC 3078
MPPE V2 56 (RFC 3078)	MPPE Version 2 mit 56-Bit-Schlüssel gemäß RFC 3078
MPPE V2 128 (RFC 3078)	MPPE Version 2 mit 128-Bit-Schlüssel gemäß RFC 3078
MPPE V1 40 only	Ausschließlich MPPE Version 1 mit 40-Bit-Schlüssel
MPPE V1 56 only	Ausschließlich MPPE Version 1 mit 56-Bit-Schlüssel
MPPE V1 128 only	Ausschließlich MPPE Version 1 mit 128-Bit-Schlüssel
DES 56	DES mit 56-Bit-Schlüssel
3DES 168	Triple DES mit 168-Bit-Schlüssel
Blowfish 56	Blowfish mit 56-Bit-Schlüssel
Blowfish 168	Blowfish mit 168-Bit-Schlüssel
none	keine Verschlüsselung

Tabelle 1-3: Auswahlmöglichkeiten von ***ENCRYPTION***

Diese Werte sind nur verfügbar, wenn unter ***ENCAPSULATION*** *PPP*, *Async PPP over X.75*, *Async PPP* over *X.75*/*T.70*/*BTX*, *Async PPP* over *V.120 (HSCSD)* oder *X.25_PPP* ausgewählt wurde.

2 Untermenü *PPP*

Im folgenden wird das Untermenü *PPP* beschrieben.

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

  Authentication               CHAP + PAP
  Partner PPP ID
  Local PPP ID                 x2200
  PPP Password

  Keepalives                   off
  Link Quality Monitoring      off


              OK                                CANCEL
```

Das Menü ***WAN PARTNER*** ➜ ***PPP*** enthält allgemeingültige ➤➤ **PPP**-Einstellungen, z. B. "Authentication Protocol", die sich auf den zu konfigurierenden WAN Partner beziehen. Mit diesen Einstellungen führt das Gateway mit eingehenden Rufen eine Authentisierungsverhandlung aus, wenn er die "Calling Party Number" nicht identifizieren kann (z. B. weil der Anruf über eine analoge Leitung eingeht, die die "Calling Party Number" nicht signalisiert).

Das Untermenü ***PPP*** besteht aus folgenden Feldern:

Feld	Wert
Authentication	Authentisierungsprotokoll. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten im Feld Authentication” auf Seite 11.
Partner PPP ID	Kennung des WAN Partners.
Local PPP ID	Kennung Ihres Gateways.
PPP Password	Passwort.

Feld	Wert
Keepalives	Aktiviert Keepalive-Pakete zur Überprüfung der Erreichbarkeit der PPP-Gegenstelle. Mögliche Werte: ■ *off* (Standardwert für Wählverbindung) ■ *on* (Standardwert für Festverbindung)
Link Qualitiy Monitoring	Aktiviert PPP Link Quality Monitoring nach RFC 1989. Mögliche Werte: ■ *off* (Standardwert) ■ *on* Nur notwendig in Ausnahmefällen, z. B. mit Nokia Communicator.

Tabelle 2-1: Felder im Untermenü ***PPP***

Das Feld ***AUTHENTICATION*** enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
PAP	Nur ➤➤ **PAP** (PPP Password Authentication Protocol) ausführen, Paßwort wird unverschlüsselt übertragen.
CHAP	Nur ➤➤ **CHAP** (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Paßwort wird verschlüsselt übertragen.
CHAP + PAP	Vorrangig CHAP, sonst PAP ausführen.
MS-CHAP	Nur MS-CHAP (MS Challenge Handshake Authentication Protocol) ausführen.
CHAP + PAP + MS-CHAP	Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom WAN Partner geforderte Authentisierungsprotokoll ausführen.
MS-CHAP V2	Nur MS-CHAP Version 2 ausführen.
none	Kein PPP-Authentisierungsprotokoll ausführen.

Tabelle 2-2: Auswahlmöglichkeiten im Feld ***AUTHENTICATION***

3 Untermenü *ADVANCED SETTINGS*

Im folgenden werden die Felder des Untermenüs *ADVANCED SETTINGS* beschrieben.

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

Spezielle Funktionen für ➤➤ **WAN Partner** ermöglichen, die Eigenschaften für Verbindungen zu WAN Partnern individuell festzulegen. Die einzelnen Konfigurationsoptionen werden für jeden WAN Partner separat eingestellt.

Callback Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann für jeden WAN Partner der Callback-Mechanismus verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufende eindeutig identifiziert wurde. Das Gateway kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch sich bei einem WAN Partner einwählen und dann einen Rückruf erwarten.

Die Identifizierung kann aufgrund der Calling Party's Number oder aufgrund der PAP/CHAP/MS-CHAP-Authentisierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party's Number über den ISDN-D-Kanal übermittelt wird, im zweiten Fall mit Rufannahme.

Shorthold festlegen

Der Shorthold wird festgelegt, um Gebühren zu sparen. Das Gateway bricht dann die ISDN-Verbindung ab, wenn keine Daten mehr fließen. Mit statischem bzw. dynamischem Shorthold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) das Gateway die ISDN-Verbindung abbauen soll.

Statisch

Mit statischem ➤➤ **Shorthold** legen Sie genau fest, wieviel Zeit zwischen Übertragung des letzten ➤➤ **Datenpakets** und Abbau der ISDN-Verbindung vergehen soll. Sie geben einen festen Zeitraum in Sekunden ein.

Dynamisch

Mit dynamischem Shorthold definieren Sie keinen festen Zeitraum, sondern berücksichtigen die Länge der ISDN-Gebührenintervalle. Der dynamische Shorthold orientiert sich dabei am AOCD ("advice of charge during the call", Übermittlung der Gebühreninformationen während der Verbindung).

Bei Festlegung des dynamischen Shortholds geben Sie an, wieviel Zeit nach dem letzten Datenfluß vergehen soll, bis die Verbindung abgebrochen wird. Dabei geben Sie eine Prozentzahl ein, die sich auf das letzte Gebührenintervall bezieht. Somit kann der Wert von ***IDLE FOR DYNAMIC SHORT HOLD*** sich verändern, so wie auch die Länge des Gebührenintervalls sich verändert (nach Tageszeit, Wochenende/Wochentag, usw.). Wenn Sie z. B. 50% eingeben, dann beträgt ***IDLE FOR DYNAMIC SHORT HOLD*** 60 Sekunden, wenn das vorhergehende Gebührenintervall 120 Sekunden lang war und 300 Sekunden, wenn das vorhergehende Gebührenintervall 600 Sekunden lang war. Die Verbindung wird nach Ablauf von ***IDLE FOR DYNAMIC SHORT HOLD*** und kurz vor Beginn des nächsten Gebührenintervalls beendet.

Delay after Connection Failure

Mit dieser Funktion richten Sie eine Wartezeit nach fehlgeschlagenem Verbindungsversuch durch das Gateway ein.

Layer 1 Protocol

Sie können das Layer 1 Protocol des ISDN-➤➤ **B-Kanals**, das das Gateway für Verbindungen zum WAN Partner nutzen soll, definieren. Voreingestellt ist das Protokoll für ISDN-Datenverbindungen mit 64 kBit/s, dem Standardwert des B-Kanals. Ändern Sie die Einstellung nur, wenn dies ausdrücklich erforderlich ist.

Channel-Bundling

Das Gateway unterstützt dynamische und statische ➤➤ **Kanalbündelung** für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch

Dynamische Kanalbündelung bedeutet, daß das Gateway bei Bedarf, also bei großen Datenmengen, weitere ➤➤ **ISDN**-B-Kanäle für Verbindungen mit dem WAN Partner zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen ➤➤ **B-Kanäle** wieder geschlossen.

Statisch

Bei statischer Kanalbündelung legen Sie von vorneherein fest, wie viele B-Kanäle das Gateway für Verbindungen mit dem WAN Partner nutzen soll, unabhängig von der übertragenen Datenmenge.

Die Konfiguration erfolgt im Menü ***WAN Partner*** ➜ ***Advanced Settings***.

Das Menü ***Advanced Settings*** besteht aus folgenden Feldern:

Feld	Wert
Callback	Aktiviert die Funktion Callback. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Callback” auf Seite 18
Static Short Hold (sec)	Inaktivitätsintervall in Sekunden für statischen Shorthold. Beispielwerte für Fernverbindungen: *60*, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD), sonst *20*.
Idle for Dynamic Short Hold (%)	Inaktivitätsintervall in Prozent für dynamischen Shorthold. Nur wirksam, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD).
Delay after Connection Failure (sec)	Blocktimer. Gibt an, für wie viele Sekunden nach einem fehlgeschlagenen Verbindungsaufbau kein erneuter Versuch durch das **VPN Access Gateway** unternommen wird.

Feld	Wert
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol das **VPN Access Gateway** nutzen soll. Diese Einstellung gilt nur für ausgehende Rufe an den WAN Partner und für eingehende Rufe vom WAN Partner, wenn sie anhand der Calling Party's Number identifiziert werden konnten. Mögliche Werte: siehe Tabelle "Auswahlmöglichkeiten von Layer 1 Protocol" auf Seite 19
Channel-Bundling	Legt fest, ob bzw. welche Art von Kanalbündelung für Verbindungen mit dem WAN Partner genutzt werden soll. Mögliche Werte: ■ *no:* Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. ■ *static:* Dynamische Kanalbündelung. ■ *dynamic:* Statische Kanalbündelung.
Total Number of Channels	Bei dynamischer Kanalbündelung: Definiert die maximale Anzahl der B-Kanäle, die geöffnet werden dürfen. Bei statischer Kanalbündelung: Definiert die Anzahl der B-Kanäle, die während der gesamten Verbindungsdauer geöffnet sind.
Remote X.25 Address	X.25-Zieladresse. Erscheint nur, wenn unter ***LAYER 1 PROTOCOL*** *AO/DI* ausgewählt ist.

Feld	Wert
Special Interface Types	Diese Option definiert den Typ des Interfaces genauer. Mögliche Werte: ■ *none*: Kein spezieller Typ ausgewählt. ■ *dialin only*: Das Interface wird nur für eingehende Wählverbindungen verwendet. ■ *Call-by-Call (dialin only)*: Das Interface wird als Multi-User WAN Partner definiert, d.h. mehrer Clients wählen sich mit gleichem Username und Passwort ein. Nur sinnvoll, wenn ***WAN Partner*** ➜ ***IP*** ➜ ***Basic Settings*** ➜ ***IP Transit Network*** auf *dynamic server* gesetzt ist.

Tabelle 3-1: Felder im Menü ***Advanced Settings***

Callback enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
no	**VPN Access Gateway** führt keinen Rückruf aus.
expected (awaiting callback)	**VPN Access Gateway** ruft den WAN Partner an, um den Callback zu initiieren.
yes (PPP negotiation)	**VPN Access Gateway** ruft zurück mit der Rufnummer, die für den WAN Partner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP Verhandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheitsgründen möglichst zu vermeiden. Bei der Anbindung von Microsoft-➤➤ **Clients** über DFÜ-Netzwerk ist derzeit aber keine Alternative verfügbar.

Wert	Bedeutung
yes (delayed, CLID only)	**VPN Access Gateway** ruft nach ca. vier Sekunden zurück, wenn Ihr Gateway vom WAN Partner dazu aufgefordert wird.
yes (PPP negotiation, callback optional)	Wie *yes (PPP negotiation)* mit Abbruchoption. Der Microsoft-Client hat hier die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zum **VPN Access Gateway** ohne Callback aufrechtzuerhalten. Dies wird erreicht, indem das erscheinende Dialogfenster mit **CANCEL** geschlossen wird. Ausnahme: Wenn der einwählende WAN Partner Windows NT nutzt und seine Rufnummer auf dem **VPN Access Gateway** eingetragen ist, kann diese Abbruchoption nicht genutzt werden!
yes	**VPN Access Gateway** ruft sofort zurück, wenn Ihr Gateway vom WAN Partner dazu aufgefordert wird.

Tabelle 3-2: Auswahlmöglichkeiten von ***CALLBACK***

LAYER 1 PROTOCOL enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
ISDN 64 kbps	Für ISDN-Datenverbindungen mit 64 kBit/s. Dies ist der Standardwert.
ISDN 56 kbps	Für ISDN-Datenverbindungen mit 56 kBit/s.

Wert	Bedeutung
Modem	(nur nutzbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen für Modemprofil 1, die im Menü ***MODEM*** ➜ ***PROFILE CONFIGURATION*** ➜ ***PROFILE 1*** getroffen wurden.
DOVB	Data transmission Over Voice Bearer – nützlich z. B. in den USA, wo Sprachverbindungen manchmal billiger sind als Datenverbindungen.
V.110 (1200 ... 38400)	Für GSM-Verbindungen mit V.110 und mit Bit-Raten von 1200 Bit/s, 2400 Bit/s,..., 38400 Bit/s.
Modem Profile 1 ... 8	(nur verfügbar bei eingebauter Erweiterungskarte mit Ressourcenkarte mit Digitalmodems) Weist eingehende analoge Rufe dem Dienst PPP-Routing zu. Das digitale Modem auf der Ressourcenkarte, das diesen Ruf entgegennimmt, verwendet die Einstellungen für Modemprofile 1... 8, die im Menü ***MODEM*** ➜ ***PROFILE CONFIGURATION*** ➜ ***PROFILE 1...8*** getroffen wurden.
PPP over Ethernet (PPPoE)	Für Verbindungen mit xDSL (siehe Kapitel 6.2.3, Seite 138).
AO/DI	Für die Nutzung von Always On/Dynamic ISDN (AO/DI, siehe Kapitel 7.2.4, Seite 198).
PPP over PPTP	Für Verbindungen mit xDSL z. B. in Österreich (siehe "Beispiel 2: Telekom Austria (High-Speed-Internet-Anschluß)", Seite 144.

Tabelle 3-3: Auswahlmöglichkeiten von ***LAYER 1 PROTOCOL***

3.1 Untermenü *EXTENDED INTERFACE SETTINGS (OPTIONAL)*

Im folgenden werden die Felder des Untermenüs *EXTENDED INTERFACE SETTINGS* beschrieben.

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

   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
```

In dem Untermenü ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS*** können zusätzliche Einstellungen zur Funktion Bandwidth On Demand (=BOD) vorgenommen werden.

Das Menü ***EXTENDED INTERFACE SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
Mode	Legt fest, welcher Modus für BOD verwendet wird. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Mode” auf Seite 27.

Feld	Wert
Line Utilization Weighting	Legt fest, wie die Auslastung der Verbindung berechnet wird. Mögliche Werte: ■ *equal*: Für die Berechnung werden alle gemessenen Werte für den Durchsatz innerhalb von ***LINE UTILIZATION SAMPLE (SEC)*** gleich gewichtet (Standardwert). ■ *proportional*: Für die Berechnung werden die zuletzt gemessenen Werte für den Durchsatz stärker gewichtet. D. h. die Berechnung wird am stärksten von den innerhalb von ***LINE UTILIZATION SAMPLE (SEC)*** zuletzt gemessenen Werten beeinflußt.
Line Utilization Sample (sec)	Zeitintervall in Sekunden. Durchsatzmessungen innerhalb von ***LINE UTILIZATION SAMPLE (SEC)*** gehen in die Berechnung der Auslastung einer Verbindung ein. Mögliche Werte: *5* bis *300* (Standardwert: *5*).
Gear Up Threshold	Auslastung, ab der bei einer Verbindung ein weiterer B-Kanal zugeschaltet wird.
Gear Down Threshold	B-Kanäle werden weggeschaltet, bis die verbleibenden Kanäle mindestens den hier verbleibenden Auslastungsgrad in Prozent aufweisen.
D-Channel Queue Length	(nur bei ***LAYER 1 PROTOCOL*** = *AO/DI* im Menü ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS***) Schwellwert für die im D-Kanal angesammelte Anzahl von Bytes, ab der in den B-Kanal-Modus gewechselt werden soll (siehe Kapitel 7.2.4, Seite 198).

Feld	Wert
Maximum Number of Dialup Channels	Maximal erlaubte Anzahl der Kanäle, die für Wählverbindungen geöffnet werden. Der Wert wird an dieser Stelle nur angezeigt, eingestellt wird er im Menü ***WAN PARTNER*** ➜ ***EDIT*** ➜ ***ADVANCED SETTINGS*** unter ***TOTAL NUMBER OF CHANNELS***.
Encryption Key Negotiation	Definiert, ob ein Schlüssel für die Verbindung zum WAN Partner automatisch generiert oder statisch definiert wird. Mögliche Werte: ■ *authentication* (Standardwert): Schlüssel wird vom **VPN Access Gateway** automatisch generiert. ■ *static*: Schlüssel wird statisch definiert und muß unter ***ENCRYPTION KEY (TX)*** bzw. ***ENCRYPTION KEY (RX)*** eingetragen werden.
Encryption Key (TX)	(nur bei ***ENCRYPTION KEY NEGOTIATION*** = *static*) Schlüssel (im hexadezimalen Format) zur Verschlüsselung ausgehender Daten (muß mit dem Eintrag unter ***ENCRYPTION KEY (RX)*** beim Verbindungspartner übereinstimmen).
Encryption Key (RX)	(nur bei ***ENCRYPTION KEY NEGOTIATIOn*** = *static*) Schlüssel (im hexadezimalen Format) zur Verschlüsselung eingehender Daten (muß mit dem Eintrag unter ***ENCRYPTION KEY (TX)*** beim Verbindungspartner übereinstimmen).

Tabelle 3-4: Felder im Untermenü ***EXTENDED INTERFACE SETTINGS***

MODE besteht aus folgenden Auswahlmöglichkeiten:

Wert	Bedeutung
Bandwidth On Demand Disabled	Deaktiviert BOD, es werden keine zusätzlichen Kanäle geöffnet (Standardwert).

Wert	Bedeutung
Bandwidth On Demand Enabled	(Nur bei Wählverbindungen) Aktiviert BOD, es können zusätzliche Kanäle geöffnet werden. Der Verbindungspartner, der die Verbindung initiiert hat, öffnet die zusätzlichen Kanäle.
BAP, Active Mode	(Bandwidth Allocation Protocol) Notwendig für AO/DI (Always On/Dynamic ISDN) Funktion. Im Bandwidth Allocation Protocol (BAP) gibt es drei verschiedene Modi für die Aushandlung einer Brandbreitenänderung. Im Active Mode verhält sich dieses wie folgt: ■ Call Request: Einer der beiden Kommunikationspartner will einen zweiten B-Kanal hinzufügen; wird ausgelöst, aber nicht angenommen. ■ Callback Request: Das entfernte Terminal wird aufgefordert, einen B-Kanal hinzuzufügen; wird ausgelöst, aber nicht angenommen. ■ Link Drop Request: Ein Kommunikationspartner will einen B-Kanal schliessen; das Schliessen wird ausgelöst, aber nicht angenommen.

Wert	Bedeutung
BAP, Passive Mode	BAP verhält sich im Passive Mode wie folgt: ■ Call Request: Einer der beiden Kommunikationspartner will einen zweiten B-Kanal hinzufügen; wird angenommen. ■ Callback Request: Das entfernte Terminal wird aufgefordert, einen B-Kanal hinzuzufügen; wird ausgelöst. ■ Link Drop Request: Ein Kommunikationspartner will einen B-Kanal schliessen; das Schliessen wird ausgelöst oder angenommen.
BAP, Active and Passive Mode	BAP verhält sich in Active oder Passive Mode wie folgt: ■ Call Request: Einer der beiden Kommunikationspartner will einen zweiten B-Kanal hinzufügen; wird ausgelöst oder angenommen. ■ Callback Request: wird nicht angewendet. ■ Link Drop Request: Ein Kommunikationspartner will einen B-Kanal schliessen; das Schliessen wird ausgelöst oder angenommen.
BAP, Client Active Mode	BAP verhält sich im Client Active Mode wie folgt: Der Partner, der die Verbindungsaufbau initiiert hat, ist im Active Mode (siehe ***BAP, ACTIVE MODE***) und der Partner, der den Anruf angenommen hat, ist im Passive Mode (siehe ***BAP, PASSIVE MODE***).

Wert	Bedeutung
BAP, Dialup Client Mode	(Nur bei Wählverbindungen) Dieser Wert weist dem Interface die Client-Rolle zu. In diesem Szenario ist der Client der aktive Partner, Kontrolle und Verantwortlichkeit liegen bei ihm (Kosten für Kanalbündelung). Es wird erwartet, dass die Zentralseite alle anfragen annimmt, die mit der WAN Partner Konfiguration auf dem Gateway der Zentralseite übereinstimmt. BAP verhält sich im Dialup Client Mode wie folgt: ■ Call Request: Der Client will einen B-Kanal hinzufügen; wird ausgelöst. ■ Callback Request: Das entfernte Terminal (Server) wird aufgefordert einen B-Kanal hinzuzufügen (eigenständig); das entfernte Terminal sendet dann einen Callback Request. ■ Link Drop Request: Ein Kommunikationspartner will einen B-Kanal schliessen; das Schliessen wird ausgelöst oder angenommen. Der ISP verteilt einkommende Rufe auf mehrere Gateways. Diese Einstellungen stellt für die Clients Kanalbündelung sicher.

Wert	Bedeutung
BAP, Dialup Server Mode	(Nur für Wahlverbindungen) Dieser Wert weist dem Interface die Server-Rolle zu. In diesem Szenario ist der Client der aktive Partner, Kontrolle und Verantwortlichkeit liegen bei ihm (Kosten für Kanalbündelung). Es wird erwartet, dass die Zentralseite alle anfragen annimmt, die mit der WAN Partner Konfiguration auf dem Gateway der Zentralseite übereinstimmt. BAP verhält sich im Dialup Client Mode wie folgt: ■ Call Request: Der Client will einen B-Kanal hinzufügen; wird ausgelöst. ■ Callback Request: Das entfernte Terminal (Server) wird aufgefordert einen B-Kanal hinzuzufügen (eigenständig); das entfernte Terminal sendet dann einen Callback Request. ■ Ein Kommunikationspartner will einen B-Kanal schliessen; das Schliessen wird angenommen. Der ISP verteilt einkommende Rufe auf mehrere Gateways. Diese Einstellungen stellt für die Clients Kanalbündelung sicher.
Backup	(Nur bei Festverbindungen) Die Backup-Verbindung wird aktiviert, falls die Festverbindung ausfällt. Wenn die Festverbindung wieder verfügbar ist, wird die Backup-Verbindung abgebaut. BOD ist auch für diesen Modus verfügbar, falls für ***MAXIMUM NUMBER OF DIALUP CHANNELS*** ein Wert > *1* verwendet wird.

Wert	Bedeutung
Bandwidth On Demand Active	(Nur bei Festverbindungen) Ermöglicht BOD und definiert den aktiven Partner. Nur einer der Verbindungspartner sollte als aktiver Partner konfiguriert sein. Diese Seite aktiviert dann bei Bedarf das Zu- und Abschalten von zusätzlichen B-Kanälen.
Bandwidth On Demand Passive	(Nur bei Festverbindungen) Ermöglicht BOD und definiert den passiven Partner. Diese Seite aktiviert kein Zu- und Abschalten von zusätzlichen Kanälen.

Tabelle 3-5: Auswahlmöglichkeiten von ***MODE***

4 Untermenü *WAN NUMBERS*

Im folgenden werden die Felder des Untermenüs *WAN NUMBERS* beschrieben.

In dem Menü ***WAN PARTNER*** ➜ ***WAN NUMBERS*** sind die aktuell eingetragenen Rufnummern des WAN Partners aufgelistet. Weitere Nummern werden über die Schaltfläche ***ADD*** hinzugefügt. Bestehende Einträge werden durch Auswahl des jeweiligen Listeneintrags bearbeitet.

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[WAN][EDIT][WAN NUMBERS][ADD]: Add or Change                MyGateway
                               WAN Numbers (test)

 Number
 Direction                        outgoing

 Advanced Settings >

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


            SAVE                                    CANCEL
```

Das Menü ***WAN NUMBERS*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Number	Rufnummer des WAN Partners.

Feld	Wert
Direction	Definiert, ob ***NUMBER*** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte: ■ *outgoing*: Für ausgehende Rufe, wenn Sie sich beim WAN Partner einwählen wollen. ■ *both (CLID)*: Für eingehende und ausgehende Rufe. ■ *incoming (CLID):* Für eingehende Rufe, wenn der WAN Partner sich bei Ihrem Gateway einwählen soll.
ISDN Ports to use	(Nur mit ISDN-Erweiterungskarten) Definiert die zu verwendenden ISDN-Ports. ■ Slot 0 Auxiliary: kein Eintrag oder *x* ■ Slot 0 ISDN S0: kein Eintrag oder *x*

Tabelle 4-1: Felder im Menü ***WAN NUMBERS***

4.1 Untermenü *ADVANCED SETTINGS*

Im folgenden wird das Untermenü *ADVANCED SETTINGS* beschrieben.

Das **VPN Access Gateway** unterstützt die Nutzung des Dienstmerkmals "Geschlossene Benutzergruppe", das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluß beantragen können. Damit wird die externe/interne Erreichbarkeit durch die Vermittlungsstellen überwacht und geregelt.

Wenn keine "Geschlossene Benutzergruppe" definiert ist, steht im Feld ***CLOSED USER GROUP*** der Wert *none*. Um eine Geschlossene Benutzergruppe für einen WAN Partner zu aktivieren, wählen Sie *specify*. In das sich öffenenden Feld wird der CUG-Index eingetragen. Informationen zu CUG erhalten Sie von Ihrer Telefongesellschaft.

5 Untermenü *IP*

Im folgenden wird das Untermenü *IP* beschrieben.

In dem Untermenü ***WAN PARTNER*** ➜ ***IP*** werden Routing-Einstellungen spezifisch für einen WAN Partner vorgenommen.

Das Untermenü ***IP*** besteht aus folgenden weiteren Untermenüs:

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

5.1 Untermenü *BASIC IP-SETTINGS*

Im folgenden werden die Felder des Untermenüs *BASIC IP-SETTINGS* beschrieben.

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

 IP Transit Network                    yes


 Local IP Address                      1.1.1.1
 Partner IP Address


 Default Route                         no

 Remote IP Address                     1.2.4.0
 Remote Netmask                        255.255.255.128


          SAVE                                CANCEL
```

Damit IP-Datagramme zwischen zwei entfernten LANs übertragen werden können, muß das Gateway die Route zu dem jeweiligen Zielnetz kennen. In diesem Menü können Sie die grundlegende Route festlegen oder eine Default Route zum Partner Gateway generieren (d.h. alle IP Pakete mit unbekannter Ziel IP-Adresse werden zum Partner Gateway gesendet).

Das Menü ***BASIC IP-SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
IP Transit Network	Legt fest, ob Ihr Gateway ein Transitnetzwerk zum WAN Partner aufbaut. Mögliche Werte: ■ *yes*: Das Transitnetzwerk wird verwendet. ■ *no*: Es wird kein Transitwetzwerk verwendet. ■ *dynamic client*: Ihr Gateway erhält die IP-Adresse dynamisch. ■ *dynamic server*: Ihr Gateway weist einwählenden Clients IP-Adressen zu.
Local IP Address	IP-Adresse Ihres Gateways. Im Normalfall müssen Sie hier keinen Eintrag machen, außer Sie richten für einen Ihrer WAN Partner ein Transitnetzwerk ein.
Partner IP Address	Nur für den Wert *yes* für ***IP TRANSIT NETWORK***. WAN-IP-Adresse des WAN Partners im Transitnetzwerk.

Feld	Wert
Enable NAT	Nur für den Wert *dynamic client* für ***IP TRANSIT NETWORK***. Mögliche Werte: ■ *yes*: NAT ist für diesen WAN Partner aktiviert. ■ *no*: NAT ist für diesen WAN Partner deaktiviert. Die Einstellungen in diesem Menü entsprechen der NAT-Aktivierung im Menü ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT***.
Default Route	Nur für den Wert *dynamic client* für ***IP TRANSIT NETWORK***. Mögliche Werte: ■ *yes*: Route zu diesem WAN Partner wird als Default-Route festgelegt. ■ *no*: Route zu diesem WAN Partner wird nicht als Default-Route festgelegt.
Remote IP Address	Nur für den Wert *yes* oder *no* für ***IP TRANSIT NETWORK***. IP-Adresse des LAN des WAN Partners.
Remote Netmask	Nur für den Wert *yes* oder *no* für ***IP TRANSIT NETWORK***. Netzmaske des LAN des WAN Partners. Wenn Sie keinen Eintrag machen, trägt Ihr Gateway eine Standard-Netzmaske für die unter Partner's LAN IP Address verwendete Netzklasse ein.

Tabelle 5-1: Felder im Menü ***BASIC IP-SETTINGS***

5.2 Untermenü *MORE ROUTING*

Im folgenden werden die Felder des Untermenüs *MORE ROUTING* beschrieben.

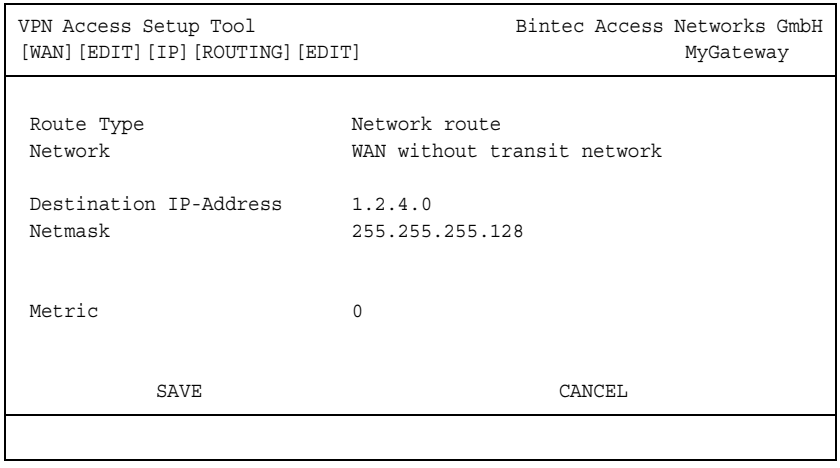
Wenn für einen spezifischen WAN Partner eine Route in ***BASIC IP-SETTINGS*** eingegeben wurde, wird automatisch ein Routing-Eintrag in der Routing-Tabelle Ihres Gateways erzeugt. Im Menü ***WAN PARTNER*** ➜ ***IP*** erscheint das Untermenü ***MORE ROUTING***. In diesem Menü können Sie die Routing-Einträge eines spezifischen WAN Partners ändern und weitere hinzufügen. Für die Verbindung zu Ihrem Internet-Service-Provider sollten Sie immer eine sogenannte Default-Route einrichten.

Im Menü ***IP*** ➜ ***MORE ROUTING*** sind alle eingetragenen IP-Routen aufgelistet:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[WAN][ADD][IP][ROUTING]: IP Routing                                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
 1.5.3.0     1.12.4.1   255.255.255.128 GS    1     new         loc
 1.12.4.1    1.12.4.1   255.255.255.255 H     0     new         loc



   ADD              ADDEXT            DELETE             EXIT
```

Unter ***FLAGS*** wird der aktuelle Status (*Up*– Aktiv, *Dormant*– Ruhend, *Blocked* – Gesperrt) und die Art der Route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*) angezeigt. Unter ***PRO*** wird angezeigt, mit welchem Protokoll Ihr Gateway den Routing-Eintrag "gelernt" hat.

Weitere Routen werden im Menü ***WAN PARTNER*** ➜ ***IP*** ➜ ***MORE ROUTING*** ➜ ***ADD*** hinzugefügt. Bestehende Einträge können bearbeitet werden, indem der gewünschte Listeneintrag ausgewählt und mit der Eingabetaste bestätigt wird.



Das Menü ***MORE ROUTING*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route*: Route zu einem einzelnen Host ■ *Network route*: Route zu einem Netzwerk ■ *Default route*: Wird nur benutzt, wenn keine andere passende Route verfügbar ist
Network	Definiert die Art der Verbindung (LAN, WAN). Mögliche Werte, siehe Tabelle “Auswahlmöglichkeiten im Feld Network” auf Seite 36.
Destination IP-Address	Nur für ***ROUTE TYPE*** *Host route* oder *Network route*. IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Netzmaske des Partner-LANs (nur möglich bei ***ROUTE TYPE*** = *Network route*. Wenn kein Eintrag erfolgt, benutzt das Gateway eine Standardnetzmaske).

Feld	Wert
Partner interface	WAN Partner bzw. Schnittstelle (nur möglich bei ***NETWORK*** = *WAN without transit network*).
Gateway IP-Address	Nur für ***NETWORK*** *LAN* oder *WAN with transit network*. IP-Adresse des Hosts, an den Ihr Gateway die IP-Pakete weitergeben soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*).

Tabelle 5-2: Felder im Menü ***MORE ROUTING***

NETWORK enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
LAN	Route zu einem Ziel-Host oder -LAN, das über den LAN-Anschluß Ihres Gateways zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN Partner ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks zu erreichen sind.
WAN with transit network	Route zu einem Ziel-Host oder -LAN, welche über einen WAN Partner nur über ein Transitnetzwerk zu erreichen sind.
Refuse	Ihr Gateway verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, daß das Ziel des Paketes unerreichbar ist.
Ignore	Ihr Gateway verwirft Datenpakete, die diese Route benutzen, ohne eine Statusmeldung zu senden.

Tabelle 5-3: Auswahlmöglichkeiten im Feld ***NETWORK***

Um Einträge für Extended Routing (Erweitertes IP-Routing) zu erzeugen, betätigen Sie die Schaltfläche ***ADDEXT*** und öffnen damit das entsprechende Menü.

Ergänzend zu der normalen Routing-Tabelle kann das **VPN Access Gateway** auch Routing-Entscheidungen aufgrund einer zusätzlichen Tabelle, der Extended-Routing-Tabelle, treffen (Erweitertes IP-Routing). Dabei kann das **VPN Access Gateway** neben der Quell- und Zieladresse u. a. auch das Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und den Status der Ziel-Schnittstelle in die Entscheidung mit einbeziehen. Wenn Einträge in der Extended-Routing-Tabelle stehen, werden diese gegenüber den Einträgen in der normalen Routing-Tabelle bevorzugt behandelt.

Beispiel Extended IP Routing (=XIPR) ist z. B. dann nützlich, wenn zwei Netzwerke mit einer LAN-LAN-Kopplung über ISDN verbunden sind, aber bestimmte Dienste (z. B. Telnet) nicht über eine ISDN-Wählverbindung, sondern über eine X.25-Verbindung geroutet werden sollen. Durch Eintragungen in der Extended Routing Table können Sie ermöglichen, daß ein Teil des IP-Verkehrs über die ISDN-Wählverbindung und ein Teil des IP-Verkehrs (z. B. für Telnet) über eine X.25-Verbindung läuft.

Die Konfiguration erfolgt im Setup-Tool-Menü ***WAN PARTNER ➜ IP ➜ MORE ROUTING ➜ ADDEXT***.

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[WAN][ADD][IP][ROUTING]: IP Routing <>                          MyGateway


 Route Type                  Host route
 Network                     WAN without transit network

 Destination IP-Address



 Metric                      1
 Source Interface            dont verify
 Source IP-Address
 Source Mask
 Type of Service (TOS)        00000000              TOS Mask  00000000
 Protocol                    dont verify


              SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route*: Route zu einem einzelnen Host ■ *Network route*: Route zu einem Netzwerk ■ *Default route*: Wird nur benutzt, wenn keine andere passende Route verfügbar ist
Network	Definiert die Art der Verbindung (LAN, WAN), siehe Tabelle “Auswahlmöglichkeiten im Feld Network” auf Seite 36.
Destination IP-Address	IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Netzmaske von ***Destination IP-Address***.
Partner / Interface	WAN Partner (nur möglich bei ***Network*** = *WAN without transit network*)
Mode	Definiert, wann das unter ***Partner / Interface*** gewählte Interface benutzt werden soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*).
Source Interface	Schnittstelle, über die die Datenpakete das Gateway erreichen.
Source IP-Address	Quell-IP-Adresse des Quell-Hosts bzw. -LANs.
Source Mask	Quellnetzmaske.
Type of Service (TOS)	Mögliche Werte: *0..255* als Bitfolge.
TOS Mask	Bitmaske für ***Type of Service***.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp, dont ver, icmp, ggp.*
Source Port	Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern (siehe Tabelle 9-24, Seite 360).

Feld	Wert
Destination Port	Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern (siehe Tabelle 9-24, Seite 360).

Tabelle 5-4: Felder im Menü ***ADDEXT***

Das Feld ***MODE*** enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
always	Route immer benutzen.
dialup-wait	Route benutzen, wenn das Interface "*up*" ist. Ist das Interface "*dormant*", dann wählen und warten, bis das Interface "*up*" ist. Sonst rerouten.
dialup-continue	Route benutzen, wenn das Interface "*up*" ist. Ist das Interface "*dormant*", dann wählen, aber rerouten, bis das Interface "*up*" ist. Sonst rerouten.
up-only	Route benutzen, wenn das Interface "*up*" ist. Sonst rerouten.

Tabelle 5-5: Auswahlmöglichkeiten von ***MODE***

Die Felder ***SOURCE PORT*** bzw. ***DESTINATION PORT*** enthalten folgende Auswahlmöglichkeiten:

Wert	Bedeutung
any	Das Filter paßt auf alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern.
priv (0..1023)	Port-Nummern: 0 ... 1023.
server (5000..32767)	Port-Nummern: 5000 ... 32767.
clients 1 (1024..4999)	Port-Nummern: 1024 ... 4999.

Wert	Bedeutung
clients 2 (32768..65535)	Port-Nummern: 32768 ... 65535.
unpriv (1024..65535)	Port-Nummern: 1024 ... 65535.

Tabelle 5-6: Auswahlmöglichkeiten von ***SOURCE PORT*** bzw. ***DESTINATION PORT***

5.3 Untermenü *ADVANCED SETTINGS*

Im folgenden werden die Felder des Untermenüs *ADVANCED SETTINGS* beschrieben.

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

Im Menü ***WAN PARTNER*** ➜ ***IP*** ➜ ***ADVANCED SETTINGS*** können erweiterte Routing-Einstellungen des jeweiligen WAN Partners vorgenommen werden.

Routing - Kurzbeschreibung

Im allgemeinen kann man Routing so beschreiben: Das ➤➤ **Gateway** empfängt ➤➤ **Datenpakete**, wobei in jedem Paket der Ziel-Host vermerkt ist. Aufgrund der Eintragungen in der sogenannten Routing-Tabelle (siehe Kapitel 6.3.2, Seite 165) entscheidet das Gateway, auf welchem Weg (Route) es das

Datenpaket weiterschickt, damit es möglichst schnell (mit möglichst wenigen Zwischenstationen) und günstig ans Ziel gelangt. Die Eintragungen der Routing-Tabelle können entweder statisch festgelegt werden, oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-In-formationen zwischen mehreren Gateways. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol).

RIP

Mit ➤➤ **RIP** tauschen Gateways ihre in Routing-Tabellen gespeicherten Informationen aus, indem sie in regelmäßigen Abständen miteinander kommunizieren und so gegenseitig Ihre Routing-Einträge ergänzen und erneuern. Das **VPN Access Gateway** unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

RIP wird für LAN und WAN separat konfiguriert.

Aktiv und Passiv

Man kann dabei aktive und passive Gateways unterscheiden: Aktive Gateways bieten Ihre Routing-Einträge per ➤➤ **Broadcasts** anderen Gateways an. Passive Gateways nehmen die Informationen der aktiven Gateways an und speichern sie, geben aber ihre eigenen Routing-Einträge nicht weiter. Das **VPN Access Gateway** kann beides.

WAN Partner

Wenn Sie mit einem WAN Partner Empfangen und/oder Senden von RIP-Paketen vereinbaren, kann das Gateway mit den Gateways im LAN des WAN Partners dynamisch Routing-Informationen austauschen.

Hinweis

Der Empfang von Routing-Tabellen über RIP ist eventuell eine Sicherheitslükke, da fremde Rechner bzw. Gateways die Routing-Funktionalität des **VPN Access Gateway**s verändern können.

ISDN-Verbindungen werden durch RIP-Pakete nicht aufgebaut oder gehalten.

IP Accounting

Diese Option ermöglicht die Aktivierung bzw. Deaktivierung der Erstellung von IP Accounting Meldungen für diesen WAN Partner. Wenn IP Accounting aktiviert ist, wird eine Abrechnungsmeldung generiert (und in die **biboAdmSyslogTable** eingeschrieben), welche detaillierte Informationen über die Verbingungen mit diesem WAN Partner enthält.

Back Route Verification Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion des **VPN Access Gateway**s. Wenn Back Route Verification bei einem WAN Partner aktiviert ist, werden über die Schnittstelle zum WAN Partner nur Datenpakete transportiert, die auf dem Rückweg über die gleiche Schnittstelle geroutet würden. Dadurch können Sie – auch ohne Filter – die Einspeisung von Paketen mit gefälschten IP-Adressen in Ihr LAN verhindern. Bekannte und noch unbekannte Denial-of-Service- und IP-Spoofing-Attacken können Sie damit einfach verhindern.

Route Announce Diese Option ermöglicht die Einstellung, wann die für dieses Interface definierten IP Routen propagiert werden sollen.

Proxy Arp Mit Hilfe von ➤➤ **Proxy ARP** kann das Gateway ➤➤ **ARP**-Requests aus dem eigenen LAN und aus dem LAN definierter WAN Partnern beantworten.Wenn ein Host im LAN zu einem anderen Host im LAN oder zu einem WAN Partner eine Verbindung aufbauen will, aber dessen Hardware-Adresse nicht kennt, sendet er einen sogenannten ARP-Request als ➤➤ **Broadcast** ins Netz. Wenn auf dem Gateway Proxy ARP aktiviert ist und der gewünschte Host über eine als Host-Route definierte WAN-Verbindung erreichbar ist, beantwortet das Gateway den ARP-Request mit seiner eigenen Hardware-Adresse. Dies ist für den Verbindungsaufbau ausreichend: Die ➤➤ **Datenpakete** werden an das Gateway geschickt, das sie dann an den gewünschten Host weiterleitet.

Das Menü ***ADVANCED SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
RIP Send	Ermöglicht Senden von RIP-Paketen über die Schnittstelle zum WAN Partner bzw. die LAN-Schnittstelle. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP Send und RIP Receive” auf Seite 44
RIP Receive	Ermöglicht Empfangen von RIP-Paketen über die Schnittstelle zum WAN Partner bzw. die LAN-Schnittstelle. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP Send und RIP Receive” auf Seite 44

Feld	Wert
IP Accounting	Ermöglicht Speichern von Accounting-Messages für ➤➤ **TCP-**, ➤➤ **UDP-** und ICMP-Sitzungen. Mögliche Werte: *on*, *off*.
Back Route Verify	Wenn Back Route Verification bei einem WAN-Partner aktiviert ist, werden über die Schnittstelle zum WAN Partner nur Datenpakete transportiert, die auf dem Rückweg über die gleiche Schnittstelle geroutet würden. Dadurch können Sie – auch ohne Filter – die Einspeisung von Paketen mit gefälschten IP-Adressen in Ihr LAN verhindern. Bekannte und noch unbekannte Denial-of-Service- und IP-Spoofing-Attacken können Sie damit einfach verhindern. Mögliche Werte: *on, off.*
Route Announce	Mögliche Werte: ■ *up or dormant*: Routen werden propagiert, wenn der Status *up* oder *dormant* ist. ■ *always*: Routen werden immer propagiert unabhängig vom Betriebsstatus. ■ *up only*: Routen werden nur propagiert, wenn der Status der Schnittstelle auf *up* steht.
Proxy Arp	Ermöglicht dem **VPN Access Gateway**, ARP-Requests aus dem eigenen LAN und von Hosts definierter WAN Partner zu beantworten. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Proxy Arp” auf Seite 45
Van Jacobson Header Compression	Verringert die Größe der TCP/IP Paktet. Mögliche Werte: ■ *on*: VJHC aktiviert. ■ *off* : VJHC deaktiviert.

Feld	Wert
Dynamic Name Server Negotiation	Nur bei Dynamic Name Server Negotiation. Definiert, ob das **VPN Access Gateway** IP-Adressen für ***Primary Domain Name Server, Secondary Domain Name Server, Primary WINS and Secondary WINS*** vom WAN Partner erhält oder diese zum WAN Partner schickt. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Dynamic Name Server Negotiation” auf Seite 46.

Tabelle 5-7: Felder im Menü ***Advanced Settings***

RIP Send bzw. ***RIP Receive*** enthalten folgende Auswahlmöglichkeiten:

Wert	Bedeutung
none	Nicht aktiviert.
RIP V2 multicast	Das Gateway wartet auf RIP-Pakete der Version 2 mit RIP V2 multicast Adresse.
RIP V1 triggered	RIP V1 Nachrichten werden gemäß RFC 2091 gesendet, empfangen und verarbeitet. Triggered ➤➤ **RIP**
RIP V2 triggered	RIP V2 Nachrichten werden gemäß RFC 2091 gesendet, empfangen und verarbeitet. Triggered ➤➤ **RIP**
RIP V1	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1.
RIP V2	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2.
RIP V1 + V2	Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2.

Tabelle 5-8: Auswahlmöglichkeiten von ***RIP Send*** und ***RIP Receive***

PROXY ARP enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
off	■ Deaktiviert Proxy ARP für diesen WAN Partner. ■ Deaktiviert Proxy ARP über die LAN-Schnittstelle.
on (up or dormant)	Das **VPN Access Gateway** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN Partner *up* (aktiv) oder *dormant* (ruhend) ist. Bei *dormant* beantwortet das **VPN Access Gateway** lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.
on (up only)	Das **VPN Access Gateway** beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum WAN Partner *up* (aktiv) ist, wenn also bereits eine Verbindung zum WAN Partner besteht.

Tabelle 5-9: Auswahlmöglichkeiten von ***PROXY ARP***

DYNAMIC NAME SERVER NEGOTIATION enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
off	Das **VPN Access Gateway** sendet oder beantwortet keine Anfragen für Name Server Adressen.

Wert	Bedeutung
yes	Die Antwort ist abhängig vom Modus für den Versand/Erhalt von IP-Adressen. (Einstellungnen werden in ***WAN PARTNER ➜ EDIT ➜ IP*** unter ***IP TRANSIT NETWORK*** vorgenommen): ■ Das **VPN Access Gateway** sendet Name Server Adress-Anfragen zum WAN Partner, wenn *dynamic client* ausgewählt wurde. ■ Das **VPN Access Gateway** beantwortet Name Server Adress-Anfragen vom WAN Partner, wenn *dynamic server* ausgewählt wurde. ■ Das **VPN Access Gateway** antwortet, schickt aber keine Name Server Adress-Anfragen, wenn *yes* oder *no* ausgewählt wurde.
client (receive)	**VPN Access Gateway** sendet Name Server Adress-Anfragen zum WAN Partner.
server (send)	**VPN Access Gateway** beantwortet Name Server Adress-Anfragen vom WAN Partner.

Tabelle 5-10: Auswahlmöglichkeiten von ***DYNAMIC NAME SERVER NEGOTIATION***

6 Untermenü *BRIDGE*

Im folgenden wird das Untermenü *BRIDGE* beschrieben.

Das **VPN Access Gateway** kann im Bridging-Modus betrieben werden.

Im Gegensatz zu einem ➤➤ **Router** arbeiten Bridges auf Schicht 2 des ➤➤ **OSI-Modells**, sind von höheren Protokollen unabhängig und übertragen Datenpakete anhand von ➤➤ **MAC-Adressen**. Die Datenübertragung ist transparent, d. h. die Informationen der Datenpakete werden nicht interpretiert.

Bridges werden eingesetzt, um Netze physikalisch zu entkoppeln und um den Datenverkehr im Netz einzuschränken, indem über Filterfunktionen Datenpakete nur in bestimmte Netzsegmente gelangen können.

Um das **VPN Access Gateway** im Bridging-Modus zu betreiben, wir der Wert im Feld ***ENABLE BRIDGING*** auf *yes* gestellt.

Index: WAN Partner