WAN PARTNER

Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.1

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. 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 zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications 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 **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. Funkwerk Enterprise Communications 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 Funkwerk Enterprise Communications 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 Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +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
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Menü WAN Partner 3
2 Untermenü PPP 11
3 Untermenü Advanced Settings 15
3.1 Untermenü Extended Interface Settings (optional) 22
4 Untermenü WAN Numbers 33
4.1 Untermenü Advanced Settings 36
5 Untermenü IP 37
5.1 Untermenü Basic IP-Settings 37
5.2 Untermenü More Routing 42
5.3 Untermenü Advanced Settings 48
6 Untermenü Bridge 55
Index: WAN Partner 57

1 Menü WAN Partner

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

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

   Current WAN Partner Configuration

     Partnername                Protocol            State

     Filiale                    ppp                 dormant


   ADD                DELETE              EXIT
```

Um mit Ihrem Gateway Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner als sogenannte WAN Partner auf Ihrem Gateway einrichten. Dies gilt sowohl für ausgehende Verbindungen (z.B. Ihr Gateway wählt sich bei einem WAN Partner ein), als auch für eingehende Verbindungen (z.B. 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 Ihr LAN mit einem entfernten LAN verbinden möchten, z. B. Ihr LAN (Firmenzentrale) und das LAN einer Filiale (Firmennetzanbindung), müssen Sie das entfernte LAN als WAN Partner einrichten.

Wenn Sie bei der Konfiguration der ISDN S0-Schnittstelle Ihres Gateways eine Festverbindung eingerichtet haben, wird im Menü ***WAN PARTNER*** bereits automatisch 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. ***PROTOCOL*** kann die möglichen Werte von ***ENCAPSULATION*** in der Tabelle “Mögliche Werte im Feld State” auf Seite 4 annehmen.

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

Wert	Bedeutung
up	verbunden
dormant	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich
blocked	nicht verbunden (z.B. aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ist ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich)
down	administrativ auf *down* gesetzt (deaktiviert); Verbindungsaufbau nicht möglich 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 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
```

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. In diesem Feld darf die erste Ziffer keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge ist auf maximal 25 Zeichen beschränkt.
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)* ■ *HDLC Framing (only IP)* ■ *LAPB Framing (only IP)* ■ *X.25_PPP* ■ *X.25* ■ *X.31 B-Channel* ■ *X.25 No Signalling* ■ *X.25 PAD* ■ *X.25 No Configuration* ■ *Frame Relay*

Feld	Wert
Encapsulation (Forts.)	■ *X.25 No Configuration* ■ *No Signalling* Da nicht alle Protokolle notwendigerweise von allen Bintec-Geräten unterstützt werden, prüfen Sie vor der Konfiguration zunächst die Verfügbarkeit anhand der Datenblätter für die jeweilige Gerätereihen unter www.bintec.de.
Encryption	Definiert die Art der Verschlüsselung, die für den Datenverkehr mit dem WAN Partner angewendet werden soll. Nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Encryption” auf Seite 8. Wenn ***ENCRYPTION*** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.
Compression	Legt die Art der Komprimierung fest, die für den Datenverkehr mit dem WAN Partner angewendet werden soll und ist nur aktiv, wenn es auch von der Gegenstelle unterstützt wird. Mögliche Werte: ■ *STAC, MS-STAC, MPPC:* 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. ■ V.42bis: Für ***ENCAPSULATION*** *LAPB Framing (only IP)* und *Multi-Protocol LAPB Framing* steht nur V.42bis-Komprimierung zur Verfügung.

Feld	Wert
Compression (Forts.)	■ *none* (Defaultwert) Eine Kombination von Verschlüsselung und Kompression ist nur zwischen einer (beliebigen) MPPE-Verschlüsselung und MPPC möglich. Bei ***ENCAPSULATION*** = *Multi-Protocol HDLC Framing, X.25, HDLC Framing (only IP), X31 B-Channel, X.25 No Signalling, X.25 PAD, X.25 No Configuration, Frame Relay* und *X.25 No Configuration, No Signalling* wird das Feld nicht angezeigt. (Da nicht alle Protokolle notwendigerweise von allen Bintec-Geräten unterstützt werden, prüfen Sie vor der Konfiguration zunächst die Verfügbarkeit anhand der Datenblätter für die jeweilige Gerätereihen unter www.bintec.de.)
Calling Line Identification	Zeigt an, ob Rufe von diesem WAN Partner anhand der "Calling Party Number" identifiziert werden (➤➤ **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:

Wert	Bedeutung
none (Defaultwert)	keine Verschlüsselung
MPPE 40	MPPE Version 1 und 2 mit 40-Bit-Schlüssel
MPPE V2 40	MPPE Version 2 mit 40-Bit-Schlüssel
MPPE V2 40 (RFC 3078)	MPPE Version 2 mit 40-Bit-Schlüssel gemäß RFC 3078: notwendig bei MS Clients ab Windows 2000 (evtl. sind hierbei MS Service Packs notwendig).

Wert	Bedeutung
MPPE V1 40 only	Ausschließlich MPPE Version 1 mit 40-Bit-Schlüssel
MPPE 56	MPPE Version 1 und 2 mit 56-Bit-Schlüssel
MPPE V2 56	MPPE Version 2 mit 56-Bit-Schlüssel
MPPE V2 56 (RFC 3078)	MPPE Version 2 mit 56-Bit-Schlüssel gemäß RFC 3078: notwendig bei MS Clients ab Windows 2000 (evtl. sind hierbei MS Service Packs notwendig).
MPPE V1 56 only	Ausschließlich MPPE Version 1 mit 56-Bit-Schlüssel
DES 56	DES mit 56-Bit-Schlüssel
Blowfish 56	Blowfish mit 56-Bit-Schlüssel
MPPE 128	MPPE Version 1 und 2 mit 128-Bit-Schlüssel
MPPE V2 128	MPPE Version 2 mit 128-Bit-Schlüssel
MPPE V2 128 (RFC 3078)	MPPE Version 2 mit 128-Bit-Schlüssel gemäß RFC 3078: notwendig bei MS Clients ab Windows 2000 (evtl. sind hierbei MS Service Packs notwendig).
MPPE V1 128 only	Ausschließlich MPPE Version 1 mit 128-Bit-Schlüssel
MPPE V1 128 (MS compatible mode)	MS kompatibler MPPE Version 1 mit 128 bit Modus für MS-CHAP V1 (nicht konform zu RFC 3079)
MPPE V2 128 (MS compatible mode)	MS kompatibler MPPE Version 2 mit 128 bit Modus für MS-CHAP V1 (nicht konform zu RFC 3079)
DES3 168	Triple DES mit 168-Bit-Schlüssel
Blowfish 168	Blowfish mit 168-Bit-Schlüssel

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. (Da nicht alle Protokolle notwendigerweise von allen Bintec-Geräten unterstützt werden, prüfen Sie vor der Konfiguration zunächst die Verfügbarkeit anhand der Datenblätter für die jeweilige Gerätereihen unter www.bintec.de.)

Für alle anderen Werte von ***ENCAPSULATION*** wird das Feld ***ENCRYPTION*** nicht angezeigt.

1 Menü WAN Partner

2 Untermenü PPP

Im folgenden wird das Untermenü *PPP* beschrieben.

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


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

  Keepalives                   off
  Link Quality Monitoring      off


              OK                              CANCEL
```

Das Menü ***WAN PARTNER*** ➜ ***PPP*** enthält spezifische ➤➤ **PPP**-Einstellungen, z. B. ***AUTHENTICATION***, die sich nur auf den zu konfigurierenden WAN Partner beziehen. Mit diesen Einstellungen führt das Gateway bei ausgehenden Rufen eine Authentisierungsverhandlung aus, bei eingehenden Rufen nur, wenn der WAN Partner per CLID erkannt wurde.

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

Feld	Wert
Authentication	Authentifizierungsprotokoll. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten im Feld Authentication” auf Seite 13.
Partner PPP ID	Kennung des WAN Partners.
Local PPP ID	Kennung Ihres Gateways. Defaultwert ist der Eintrag aus ***LOCAL PPP ID*** im Menü ***SYSTEM***.
PPP Password	Passwort.

Feld	Wert
Keepalives	Einstellung der Funktion PPP-Keepalive zur Überprüfung der Erreichbarkeit der PPP-Gegenstelle. Mögliche Werte: ■ *off* (Defaultwert für Wählverbindung)- deaktiviert Keepalive. ■ *on* (Defaultwert für Festverbindung) - Aktiviert Keepalive. Bei der PPP-Keepalive-Funktion wird alle drei Sekunden ein Paket zur Gegenstelle geschickt. Wenn das Paket fünf mal unbeantwortet bleibt, wird das Interface normalerweise bei Festverbindungen auf *down*, bei dialup-Verbindungen auf *dormant* gesetzt.
Link Quality Monitoring	Aktiviert PPP Link Quality Monitoring nach RFC 1989. Mögliche Werte: ■ *off* (Defaultwert) ■ *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 (Defaultwert)	Vorrangig CHAP, sonst PAP ausführen.
MS-CHAP	Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen.
CHAP + PAP + MS-CHAP	Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom WAN Partner geforderte Authentifizierungsprotokoll ausführen. (MS-CHAP Version 1 oder 2 möglich.)
MS-CHAP V2	Nur MS-CHAP Version 2 ausführen.
none	Kein PPP-Authentifizierungsprotokoll ausführen.

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

2 Untermenü PPP

3 Untermenü Advanced Settings

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][ADVANCED]: Advanced Settings (Filiale)            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 und werden im Menü ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS*** konfiguriert.

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 von einem WAN Partner einen Rückruf anfordern.

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

Short Hold festlegen

➤➤ **Short Hold** wird festgelegt, um die Verbindung bei Nichtbenutzen, d.h. wenn keine Nutzdaten mehr gesendet werden, automatisch zu trennen und so-

mit Gebühren zu sparen. Mit statischem bzw. dynamischem Short Hold legen Sie fest, nach welchem Inaktivitätsintervall (Idle Timer) das Gateway die Verbindung abbauen soll.

Statisch

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

Dynamisch (nur bei ISDN)

Mit dynamischem Short Hold definieren Sie keinen festen Zeitraum, sondern berücksichtigen die Länge der ISDN-Gebührenintervalle. Der dynamische Short Hold orientiert sich dabei am AOCD ("advice of charge during the call", Übermittlung der Gebühreninformationen während der Verbindung), der abhängig von Tageszeit, Wochenende/Wochentag ist.

Bei Festlegung des dynamischen Short Holds geben Sie an, wieviel Prozent eines Gebührenintervalls seit dem zuletzt gesendeten Nutzdatenpaket erreicht werden dürfen, bis die Verbindung abgebrochen werden kann. Allerdings wird die Verbindung erst kurz vor dem nächsten erwarteten Gebührenintervall abgebrochen. Wenn Sie z. B. 50% eingeben, dann entspricht ***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. Verwenden Sie aus Sicherheitsgründen ***Idle for Dynamic Short Hold*** nur in Verbindung mit ***Static Short Hold***.

Delay after Connection Failure

Mit dieser Funktion richten Sie eine Wartezeit für ausgehende Verbindungsversuche ein, nachdem ein Verbindungsversuch durch das Gateway fehlgeschlagen ist.

Layer 1 Protocol

Sie können das Layer 1 Protocol für ausgehende Verbindungen zum WAN Partner definieren.

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 Datenraten, 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 im Voraus fest, wie viele B-Kanäle das Gateway für Verbindungen mit dem WAN Partner nutzen soll, unabhängig von der übertragenen Datenrate.

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

Feld	Wert
Callback	Aktiviert die Funktion Callback. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Callback” auf Seite 21.
Static Short Hold (sec)	Inaktivitätsintervall in Sekunden für statischen Short Hold. Zur Verfügung stehen Werte von *-1* bis *3600* (Sekunden). Ein Wert von *-1* bedeutet, dass die Verbindung nach einem Abbruch sofort wieder aufgebaut wird, *0* deaktiviert den Shorthold. Defaultwert ist *20*. Bsp. *10* für FTP-Übertragungen *20* für LAN-zu-LAN-Übertragungen *90* für Internetverbindungen
Idle for Dynamic Short Hold (%)	Inaktivitätsintervall in Prozent des Gebührenintervalls für dynamischen Short Hold. Defaultwert ist *0*. Nur einstellen, wenn Gebühreninformationen während der Verbindung übermittelt werden (AOCD).

Feld	Wert
Delay after Connection Failure (sec)	Blocktimer. Gibt an, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch das **VPN Access** Gateway unternommen wird. Defaultwert ist *300*.
Layer 1 Protocol	Legt fest, welches Layer 1 Protocol das **VPN Access** Gateway nutzen soll. Diese Einstellung gilt für ausgehende Verbindungen zum WAN Partner und nur für eingehende Verbindungen vom WAN Partner, wenn sie anhand der Calling Party Number identifiziert werden konnten. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Layer 1 Protocol” auf Seite 22. Ändern Sie die Einstellung nur, wenn dies ausdrücklich erforderlich ist.
Channel-Bundling	Legt fest, ob bzw. welche Art von Kanalbündelung für ISDN-Verbindungen mit dem WAN Partner genutzt werden soll. Mögliche Werte: ■ *no* (Defaultwert)*:* Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. ■ *static:* Dynamische Kanalbündelung. ■ *dynamic:* Statische Kanalbündelung. Das Feld wird nicht angezeigt bei ***LAYER 1 PROTOCOL*** *= PPP over Ethernet (PPPoE), PPP over PPTP*.

Feld	Wert
Total Number of Channels	Nur bei ***CHANNEL-BUNDLING*** = *dynamic, static*. 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. Defaultwert ist *1*.
Remote X.25 Address	X.25-Zieladresse. Erscheint nur, wenn unter ***LAYER 1 PROTOCOL*** *AO/DI* ausgewählt ist. Da nicht alle Protokolle notwendigerweise von allen Bintec-Geräten unterstützt werden, prüfen Sie vor der Konfiguration zunächst die Verfügbarkeit anhand der Datenblätter für die jeweilige Gerätereihen unter www.bintec.de.
Special Interface Types	Diese Option erlaubt eine spezielle Nutzung des Interfaces. Mögliche Werte: ■ *none* (Defaultwert): Kein spezieller Typ ausgewählt. ■ *dialin only*: Das Interface wird für eingehende Wählverbindungen und für von aussen initiierten Callback verwendet. ■ *Call-by-Call (dialin only)*: Das Interface wird als Multi-User WAN Partner definiert, d.h. mehrere 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 (Defaultwert)	**VPN Access** Gateway führt keinen Rückruf aus.
expected (awaiting call-back)	**VPN Access** Gateway ruft den WAN Partner an, um einen Rückruf anzufordern.
yes (PPP negotiation)	Das **VPN Access** Gateway ruft nach einer vom Microsoft Client vorgeschlagenen Zeit (NT: 10 Sekunden, neuer Systeme: 12 Sekunden) zurück mit der Rufnummer mit ***DIRECTION*** *out-going* oder *both*, die für den WAN Partner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP Aushandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheitsgründen möglichst nicht zu verwenden. Bei der Anbindung von mobilen Microsoft-➤➤ **Clients** über DFÜ-Netzwerk ist derzeit nicht vermeidbar.
yes (delayed, CLID only)	Das **VPN Access** Gateway ruft nach ca. vier Sekunden zurück, wenn Ihr Gateway vom WAN Partner dazu aufgefordert worden ist. Nur sinnvoll bei CLID.
yes (PPP negotiation, callback optional)	Wie *yes (PPP negotiation)* mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zum **VPN Access** Gateway ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer im WAN Partner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit **CANCEL** geschlossen wird.

Wert	Bedeutung
yes	Das **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 (da nicht alle Protokolle notwendigerweise von allen Bintec-Geräten unterstützt werden, prüfen Sie vor der Konfiguration zunächst die Verfügbarkeit anhand der Datenblätter für die jeweilige Gerätereihen unter www.bintec.de.):

Wert	Bedeutung
ISDN 64 kbps (Defaultwert)	Für ISDN-Datenverbindungen mit 64 kBit/s
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

Wert	Bedeutung
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
PPP over PPTP	Für Verbindungen mit xDSL z. B. in Österreich
AO/DI	Für die Nutzung von Always On/Dynamic ISDN

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

   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*** werden per Default nur Optionen zu ***Encryption Key Negotiation*** angezeigt. Wenn ***Channel Bundling*** auf *dynamic* gesetzt wurde, erscheinen zusätzliche Einstellmöglichkeiten zur Funktion Bandwidth On Demand (=BOD). Wenn BOD im Feld ***Mode*** aktiviert wird, werden weitere Optionen sichtbar.

Nach erstmaligen Sichern der Konfiguration in diesem Menü wird die Meldung *Optional Extended Interface Settings not configured yet!* ausgeblendet und die Option **Delete Configuration** wird angezeigt.

Channel-Bundling

Die Funktion Channel-Bundling kann nur für ISDN-Verbindungen oder Festverbindungen in Verbindung mit ISDN für Bandbreitenerhöhung bzw. als Backup angewendet werden. Die Geräte der **VPN Access** Gerätereihe verfügen über verschiedene Schnittstellen. Ob Ihr Gateway über eine ISDN-Schnittstelle verfügt, entnehmen Sie bitte dem Handbuch-Teil **Technischen Daten** oder prüfen Sie die Anschlüsse am Gerät.

Falls auf der Gegenstelle Geräte anderer Fabrikate verwendet werden, stellen Sie sicher, dass diese dynamische Kanalbündelung bzw. BACP/BAP auch für Festverbindungen in Verbindung mit ISDN für Bandbreitenerhöhung bzw. als Backup unterstützen.

Das Menü ***Extended Interface Settings*** besteht aus folgenden Feldern:

Feld	Wert
Mode	Nur für ***WAN Partner*** ➜ ***Advanced Settings*** ➜ ***Channel-Bundling*** = *dynamic* Legt fest, welcher Modus für BOD verwendet wird. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Mode” auf Seite 32.
Line Utilization Weighting	Nur für ***Mode*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Legt fest, wie die Auslastung der Verbindung berechnet wird. Die Berechnung der Last erfolgt im Sekundentakt. Mögliche Werte: ■ *equal* (Defaultwert): Für die Berechnung werden alle gemessenen Werte für den Durchsatz innerhalb von ***Line Utilization Sample (sec)*** gleich gewichtet. ■ *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.

Feld	Wert
Line Utilization Sample (sec)	Nur für ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Zeitintervall in Sekunden. Durchsatzmessungen innerhalb von ***LINE UTILIZATION SAMPLE (SEC)*** gehen in die Berechnung der Auslastung einer Verbindung (was im Sekundentakt erfolgt) ein. Mögliche Werte: *5* bis *300,* Defaultwert ist *5*.
Gear Up Threshold	Nur für ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Auslastung in Prozent, ab der bei einer Verbindung ein weiterer ISDN B-Kanal zugeschaltet wird. Defaultwert ist *90*.
Gear Down Threshold	Nur für ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Ein zugeschalteter ISDN B-Kanal wird weggeschaltet, sobald sich für die verbleibende Verbindung eine prozentuale Auslastung unterhalb des hier eingestellten Wert ergibt. Defaultwert ist *80*.

Feld	Wert
D-Channel Queue Length	(nur bei ***LAYER 1 PROTOCOL*** = *AO/DI* im Menü ***WAN PARTNER*** ➜ ***ADVANCED SETTINGS***) Ob Ihr Gateway das Feature AO/DI enthält, entnehmen Sie bitte dem Datenblatt unter www.bintec.de. Nur für ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Schwellwert für die im Pufferspeicher des D-Kanals angesammelte Anzahl von Bytes, ab der in den B-Kanal- Modus gewechselt werden soll. Defaultwert ist *7500*.
Maximum Number of Dialup Channels	Nur für ***MODE*** = *Bandwidth On Demand Enabled* / *BAP, Active Mode* / *BAP, Passive Mode* / *BAP, Active and Passive Mode* / *BAP, Client Active Mode* / *BAP, Dialup Server Mode* Maximal mögliche Anzahl von ISDN B-Kanälen, die für diesen WAN Partner geöffnet werden können. Der Wert wird an dieser Stelle nur angezeigt, eingestellt wird er im Menü ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** unter ***TOTAL NUMBER OF CHANNELS***. Defaultwert ist *1*.

Feld	Wert
Encryption Key Negotiation	Definiert, ob ein Schlüssel für eine ggf. in ***WAN Partner*** ➜ ***Encryption*** aktivierte Verschlüsselung für die Verbindung zum WAN Partner automatisch generiert oder statisch definiert wird. Mögliche Werte: ■ *authentication* (Defaultwert): 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 Entschlüsselung 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** (Defaultwert).

Wert	Bedeutung
Bandwidth On Demand Enabled	(Nur bei Wählverbindungen) Aktiviert BOD; es können zusätzliche ISDN B-Kanäle geöffnet werden. Der Verbindungspartner, der die Verbindung initiiert hat, öffnet die zusätzlichen Kanäle.
BAP, Active Mode und *BAP, Passive Mode*	BAP=Bandwidth Allocation Protocol Für ***LAYER1 PROTOCOL*** = *AO/DI* (=Always On/Dynamic ISDN) muß *BAP, Active Mode* gesetzt werden. Die Funktion AO/DI ist abhängig vom Gerätetyp. Ob Ihr Gateway diese Funktion unterstützt wird, entnehmen Sie bitte dem Datenblatt auf www.bintec.de. Im Bandwidth Allocation Protocol (BAP) gibt es drei verschiedene Modi für die Aushandlung einer Brandbreitenänderung. Dabei nehmen die beiden Verhandlungspartner jeweils entgegengesetzte Rollen ein. Bei diesem Szenario muß der entfernte Verbindungspartner immer im jeweils entgegengesetzen Mode oder im *BAP, Active Mode and Passive Mode* sein. Die Verhandlungspartner verhalten sich wie folgt: ■ Call Request: Der Partner im Active Mode will einen zweiten B-Kanal hinzufügen. Er schickt einen Call Request. Ein Partner im Passive Mode nimmt ggf. den Call Request des Verhandlungspartners an. Der Partner im Active Mode öffnet daraufhin den Kanal. ■ Callback Request: Der Partner im Active Mode fordert den Partner im Passive Mode auf, einen zweiten B-Kanal hinzuzufügen. Er schickt einen Callback Request. Ein Partner im Passive Mode nimmt ggf. den Callback Request des Verhandlungspartners an und öffnet den Kanal.

Wert	Bedeutung
BAP, Active Mode und *BAP, Passive Mode* (Forts.)	■ Link Drop Request: Der Partner im Active Mode will einen B-Kanal schliessen. Er schickt einen Link Drop Request. Ein Partner im Passive Mode nimmt ggf. den Link Drop Request des Verhandlungspartners an. Daraufhin schliesst der der Partner im Active Mode den Kanal.
BAP, Active and Passive Mode	Bei dieser Option können beide Seiten sowohl den Active Mode als auch den Passive Mode übernehmen. Die Verhandlungspartner verhalten sich wie folgt: ■ Call Request: Einer der Partner will einen zweiten B-Kanal hinzufügen. Er schickt einen Call Request, der Partner nimmt den Call Request des Verhandlungspartners an. Beide Partner können sowohl den Call Request schicken als auch einen Call Request des Partners annehmen. ■ Callback Request: Einer der Partner fordert den anderen auf, einen zweiten B-Kanal hinzuzufügen. Er schickt einen Callback Request, der Partner nimmt den Callback Request des Verhandlungspartners an und öffnet den B-Kanal. Beide Partner können sowohl den Callback Request schicken als auch einen Callback Request des Partners annehmen.

Wert	Bedeutung
BAP, Active and Passive Mode (Forts.)	■ Link Drop Request: Einer der Partner will einen B-Kanal schliessen. Er schickt einen Link Drop Request, der Partner nimmt den Link Drop Request des Verhandlungspartners an. Beide Partner können sowohl den Link Drop Request schicken als auch einen Link Drop Request des Partners annehmen. Beachten Sie, dass am entfernten Gateway ebenfalls *BAP, Active and Passive Mode*, oder bei Geräten anderer Fabrikate RFC 2125 unterstützt wird und eine entsprechende Funktion aktiviert sein muß.
BAP, Client Active Mode	BAP verhält sich im Client Active Mode wie folgt: Der Partner, der den 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*). Beachten Sie, dass am entfernten Gateway ebenfalls *BAP, Client Active Mode*, oder bei Geräten anderer Fabrikate RFC 2125 unterstützt wird und eine entsprechende Funktion aktiviert sein muß.

Wert	Bedeutung
BAP, Dialup Client Mode und *BAP, Dialup Server Mode*	(nur für Wählverbindungen) Von einem ➤➤ **ISP** kann auch dann Kanalbündelung gewährleistet werden, wenn dieser die ankommenden Rufe auf mehrere Gateways verteilt: Dem Client, der sich einwählt und einen weiteren B-Kanal anfordert, wird eine bestimmte ISDN-Nummer übermittelt. Diese wird für jedes Gateway der Zentralseite individuell vergeben, so daß die Rufe mehrerer Kanäle über diese Rufnummer tatsächlich auf demselben Gateway terminiert werden. Der Aufbau des zusätzlichen B-Kanals wird durch eine Art Callback realisiert: Der Client fordert einen weiteren B-Kanal an. Daraufhin fordert die Zentralseite einen Ruf mit der individuellen Rufnummer des Gateways an, mit dem der Client bereits aktuell verbunden ist. In diesem Szenario ist der Client der aktive Teilnehmer, d. h. die Kontrolle und die Verantwortung (Kosten für Kanalbündelung) liegen bei diesem. Die Zentralseite akzeptiert alle Anfragen des Clients, solange diese in Übereinstimmung mit der WAN-Partner-Konfiguration des Gateways stehen. ■ Clientseitige Einstellung: *BAP, Dialup Client Mode* ■ Serverseitige Einstellung: *BAP, Dialup Server Mode* (zudem: Konfiguration zusätzlicher Werte wie z.B. ***BAPNUMBER*** und ***BAPLKTYPE*** in der ***PPPDIALPROFILETABLE*** über die SNMP-Shell Ihres Gateways)

Wert	Bedeutung
BAP, Dialup Client Mode und *BAP, Dialup Server Mode* (Forts.)	Auf beiden Seiten muß Kanalbündelung aktiviert sein. (siehe ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***CHANNEL BUNDLING*** auf *dynamic* oder *static* setzen) Wenn die Einwahlauthentifizierung über einen RADIUS-Server erfolgt, müssen bei der Konfiguration des RADIUS-Servers die Bintec-spezifischen Attribute verwendet werden. Dazu muß in der Users-Datei ein Eintrag angelegt werden, der die notwendigen Einträge in der ***PPPEXTIFTABLE*** erzeugt.
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. Es muß mindestens ein weiterer ISDN S0-Anschluß für Wählverbindungen zur Verfügung stehen. Über wieviele ISDN S0-Anschlüsse Ihr Gateway verfügt, entnehmen Sie dem Datenblatt unter www.bintec.de.
Bandwidth on Demand Active und *Bandwidth on Demand Passive*	(Nur bei Festverbindungen) Ermöglicht BOD. *Bandwidth on Demand Active* definiert den aktiven Partner. Diese Seite aktiviert bei Bedarf das Zu- und Abschalten von zusätzlichen B-Kanälen. *Bandwidth on Demand Passive* definiert den passiven Partner.

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

 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* (Defaultwert): 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. Die Calling Party Number des eingehenden Rufes wird mit der unter ***NUMBER*** eingetragenen Nummer verglichen. Die Calling Party Number ist in ***MONITORING & DEBUGGING*** ➜ ***ISDN MONITOR*** als ***REMOTE NUMBER*** nachzulesen.
ISDN Ports to use	(Nur bei Geräten mit ISDN S0-Anschluss. Über welche Schnittstellen Ihr Gateway verfügt entnehmen Sie bitte dem Datenblatt zu der VPN Access Gerätereihe auf www.bintec.de) 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***

Hinweis

Wenn das Gateway an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende Null bei der Einwahlnummer berücksichtigen.

Wildcards

Beim Eintragen von ***NUMBER*** können Sie entweder die Rufnummer Ziffer für Ziffer eintragen oder einzelne Ziffern oder Gruppen von Ziffern durch Wildcards ersetzen. Damit kann ***NUMBER*** für verschiedene Rufnummern zutreffen.

Die Benutzung der in der folgenden Tabelle dargestellten Wildcards wirkt sich unterschiedlich für eingehende und ausgehende Rufe aus:

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	Das Gateway akzeptiert eingehende Rufe z.b. mit:	Ausgehende Rufe, d.h. das Gateway baut eine Verbindung zum WAN-Partner auf mit
*	Entspricht einer Gruppe von keiner bis mehreren Ziffern.	Wird ignoriert.	123*	123, 1234, 123789	123
?	Entspricht genau einer Ziffer.	Wird durch 0 ersetzt.	123?	1234, 1238, 1231	1230
[a-b]	Definiert einen Bereich von passenden Ziffern.	Die erste Ziffer des definierten Bereiches wird verwendet.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Definiert einen Bereich von verbotenen Ziffern.	Die erste Ziffer nach dem definierten Bereich wird verwendet.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Entspricht einer Gruppe von optionalen Ziffern.	Wird verwendet.	{00}1234	001234 und 1234	001234

Tabelle 4-2: Wildcards für ein- und ausgehende Rufe

Hinweis

Wenn die Calling Party Number eines eingehenden Rufes sowohl mit ***NUMBER*** eines WAN-Partners mit Wildcards als auch mit ***NUMBER*** eines WAN Partners ohne Wildcards übereinstimmt, dann wird immer der Eintrag ohne Wildcards genutzt.

4.1 Untermenü Advanced Settings

Im Folgenden wird das Untermenü *WAN NUMBERS* ➜ *ADVANCED SETTINGS* beschrieben.

Das **VPN Access** Gateway unterstützt die Nutzung des Dienstemerkmals "Geschlossene Benutzergruppe", das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluß beantragen können. Damit wird die Erreichbarkeit Ihres ISDN S0-Anschlusses durch die Vermittlungsstellen überwacht und geregelt.

Wenn keine "Geschlossene Benutzergruppe" definiert ist, steht im Feld ***CLOSED USER GROUP*** (=CUG) der Wert *none* (Defaultwert). Um eine Geschlossene Benutzergruppe für einen WAN Partner zu aktivieren, wählen Sie *specify*. In das sich öffnende 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. Bei *TRANSIT NETWORK yes* wird folgendes Fenster angezeigt (mit Beispieladressen):

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

Damit IP-Datagramme zwischen zwei getrennten LANs übertragen werden können, muß das Gateway die Route zu dem jeweiligen Zielnetz kennen. In diesem Menü können Sie das grundlegende Routing für einen spezifischen WAN-Partner festlegen bzw. für diesen eine Default Route generieren.

Default Route Bei einer Default Route werden automatisch alle Daten zu diesem WAN-Partner geleitet, wenn keine andere passende Route verfügbar ist.

Wenn Sie einen Zugang zum Internet einrichten, dann tragen Sie die Route zu Ihrem Internet-Service-Provider (ISP) als Default-Route ein.

Wenn Sie z. B. eine Firmennetzanbindung machen, dann tragen Sie die Route zur Zentrale bzw. zur Filiale nur dann als Default-Route ein, wenn Sie keinen Internetzugang über Ihr Gateway einrichten.

Wenn Sie z. B. sowohl einen Zugang zum Internet, als auch eine Firmennetzanbindung einrichten, dann tragen Sie zum ISP eine Default-Route und zur Firmenzentrale eine Netzwerk-Route ein.

Sie können auf Ihrem Gateway mehrere Default-Routen eintragen, nur eine einzige aber kann jeweils wirksam sein. Achten Sie daher auf unterschiedliche Werte für ***METRIC***, wenn Sie mehrere Default Routen eintragen.

Transitnetzwerk Sie verwenden sowohl für Ihr Gateway als auch für den WAN-Partner jeweils eine zusätzliche ISDN-IP-Adresse. Damit bauen Sie während der Verbindung ein virtuelles IP-Netzwerk auf, ein sogenanntes Transitnetzwerk. Diese Einstellung benötigen Sie normalerweise nicht, nur bei manchen Spezialkonfigurationen ist sie notwendig.

Wenn in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***LAYER 1 PROTOCOL*** andere Optionen als *PPP over PPTP* gewählt wurden, besteht das Menü ***BASIC IP-SETTINGS*** aus folgenden Feldern:

Feld	Wert
IP Transit Network	Legt fest, ob Ihr Gateway ein Transitnetzwerk zum WAN Partner verwendet. Mögliche Werte: ■ *yes*: Das Transitnetzwerk wird verwendet. ■ *no* (Defaultwert): Es wird kein Transitnetzwerk verwendet. ■ *dynamic client*: Ihr Gateway erhält dynamisch eine IP-Adresse. ■ *dynamic server*: Ihr Gateway vergibt der Gegenstelle dynamisch eine IP-Adresse.
Local IP Address	Nur bei ***IP TRANSIT NETWORK*** = *yes*, *no*. ■ bei *yes* = WAN IP-Adresse Ihres Gateways ■ bei *no* = LAN IP-Adresse Ihres Gateways
Partner IP Address	Nur für den Wert *yes* für ***IP TRANSIT NETWORK***. WAN-IP-Adresse des WAN Partners im Transitnetzwerk.
Enable NAT	Nur für den Wert *dynamic client* für ***IP TRANSIT NETWORK***. Mögliche Werte: ■ *yes*: NAT ist für diesen WAN Partner aktiviert. ■ *no* (Defaultwert): NAT ist für diesen WAN Partner deaktiviert. Die Einstellungen in diesem Menü entsprechen der NAT-Aktivierung im Menü ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT***.

Feld	Wert
Default Route	Nur für den Wert *dynamic client*, *no* oder *yes* für ***IP TRANSIT NETWORK***. Mögliche Werte: ■ *yes*: Route zu diesem WAN Partner wird als Default-Route festgelegt. ■ *no* (Defaultwert): 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 LANs des WAN Partners.
Remote Netmask	Nur für den Wert *yes* oder *no* für ***IP TRANSIT NETWORK***. Netzmaske des LAN des WAN Partners.

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

Für eine xDSL-Anbindung über PPTP z.B. der Telekom Austria wird in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***LAYER 1 PROTOCOL*** die Option *PPP over PPTP* gewählt. Dann besteht das Menü ***BASIC IP-SETTINGS*** aus folgenden Feldern:

Feld	Wert
PPTP VPN Partner's IP Address	Hier tragen Sie die IP Addresse der PPTP-Gegenstelle Ihres Internet Service Providers (=ISP) ein.
via IP Interface	Dieses Feld wird angezeigt, wenn in ***PPTP VPN PARTNER'S IP ADDRESS*** eine IP Adresse eingetragen wurde. Hier wählen Sie das IP Interface aus, über das Pakete von der/zur PPTP-Gegenstelle Ihres ISPs transportiert werden.

Feld	Wert
Use Gateway	Dieses Feld wird angezeigt, wenn in ***VIA IP INTERFACE*** ein Interface bestätigt wird. Definiert, ob der PPTP-Tunnel über ein Gateway realisiert wird. Standardmässig ist hier *no* eingestellt und sollte nur in Spezialfällen geändert werden.
Gateway IP Address	Nur für ***USE GATEWAY*** = *yes* IP Addresse des durch ***USE GATEWAY*** = *yes* zwischengeschalteteten Gateways.
Local PPTP VPN IP Address	Dieses Feld wird angezeigt, wenn in ***VIA IP INTERFACE*** ein Interface bestätigt wird und ***USE GATEWAY*** = *no* gesetzt ist. IP-Adresse Ihres Gateways für die PPTP-Anbindung.
Enable NAT	Definiert, ob Network Address Translation aktiviert wird. Mögliche Werte: ■ *yes*: NAT ist für diesen WAN Partner aktiviert. ■ *no* (Defaultwert): NAT ist für diesen WAN Partner deaktiviert.
Default Route	Definiert, ob die Route zu diesem WAN Partner als Default-Route festgelegt wird. Mögliche Werte: ■ *yes*: Route zu diesem WAN Partner wird als Default-Route festgelegt. ■ *no* (Defaultwert): Route zu diesem WAN Partner wird nicht als Default-Route festgelegt.

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.

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][ADD][IP][ROUTING]: IP Routing (Filiale)                 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    Filiale    loc
 192.168.100.2 192.268.100.1 255.255.255.0  DH    1    Filiale    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.

```
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                      1

          SAVE                                CANCEL
```

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

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route* (Defaultwert): 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. Mögliche Werte, siehe Tabelle “Mögliche Einträge im Feld Network” auf Seite 44. Der angezeigte Wert kann hier nicht bearbeitet werden und ist abhängig von der Einstellung in ***IP TRANSIT NETWORK*** in ***WAN PARTNER*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***BASIC IP SETTINGS***.
Destination IP-Address	Nur für ***ROUTE TYPE*** *Host route* oder *Network route*. IP-Adresse des Ziel-Hosts oder -LANs.

Feld	Wert
Netmask	Netzmaske des Partner-LANs (nur möglich bei ***ROUTE TYPE*** = *Network route*. Wenn kein Eintrag erfolgt, benutzt das Gateway eine Standardnetzmaske).
Gateway IP-Address	Nur für ***NETWORK*** = *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*). Defaultwert ist *1*.

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

NETWORK enthält folgende mögliche Einträge:

Wert	Bedeutung
WAN without transit network	Route zu einem Ziel-Host oder -LAN, die über einen WAN Partner ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks zu erreichen sind.
WAN with transit network	Route zu einem Ziel-Host oder -LAN, die über einen WAN Partner über ein Transitnetzwerk zu erreichen sind.

Tabelle 5-3: Mögliche Einträge im Feld ***NETWORK***

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.

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

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-Tabelle 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 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
```

Das Menü enthält folgende Felder:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route* (Defaultwert): 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, siehe Tabelle “Mögliche Einträge im Feld Network” auf Seite 44. Der angezeigte Wert kann hier nicht bearbeitet werden und ist abhängig von der Einstellung in ***IP Transit Network*** in ***WAN Partner*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***Basic IP Settings***.
Destination IP-Address	Nur für ***Route Type*** = *Host route*, *Network route* IP-Adresse des Ziel-Hosts oder -LANs.
Netmask	Nur für ***Route Type*** = *Network route* Netzmaske von ***Destination IP-Address***.
Partner / Interface	Anzeige des WAN-Partners (nur möglich bei ***Network*** = *WAN without transit network*). Feld kann nicht verändert werden.
Mode	Nur möglich bei ***Network*** = *WAN without transit network*. Definiert, wann der WAN-Partner benutzt werden soll. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Mode” auf Seite 48
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*). Defaultwert ist *1*.

Feld	Wert
Source Interface	Schnittstelle, über die die Datenpakete das Gateway erreichen. Defaultwert ist *don't verify*.
Source IP-Address	Quell-IP-Adresse des Quell-Hosts bzw. -LANs.
Source Mask	Netzmaske von ***SOURCE IP-ADDRESS***
Type of Service (TOS)	Mögliche Werte: *0..255* in binärem Format.
TOS Mask	Bitmaske für ***TYPE OF SERVICE***.
Protocol	Legt das Protokoll fest. Mögliche Werte: *don't verify*, *icmp, ggp, tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp.* Defaultwert ist *don't verify*.
Source Port	Nur für ***PROTOCOL*** = *tcp, udp* Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern.
Destination Port	Nur für ***PROTOCOL*** = *tcp, udp* Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern.

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

MODE enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
always (Defaultwert)	Route immer benutzbar.
dialup-wait	Route benutzbar, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen und warten, bis das Interface "up" ist.

Wert	Bedeutung
dialup-continue	Route benutzbar, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen, und solange die Alternative Route benutzen (rerouting), bis das Interface "up" ist.
up-only	Route benutzbar, wenn das Interface "up" ist.

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

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

Wert	Bedeutung
any (Defaultwert)	Die Route 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.
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 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][IP][ADVANCED]: Advanced Settings (Filiale)        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 u.a. erweiterte Routing-Einstellungen für den jeweiligen WAN Partner vorgenommen werden.

RIP Die Eintragungen der Routing-Tabelle können entweder statisch festgelegt werden, oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Gateways. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol).

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 spei-

chern 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 Ihr Gateway mit den Gateways im LAN der Gegenstelle dynamisch Routing-Informationen austauschen.

Hinweis

Der Empfang von Routing-Tabellen über RIP kann eine Sicherheitslücke sein, da fremde Rechner bzw. Gateways die Routing-Funktionalität des **VPN Access** Gateways verändern können.

Wähl-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 Statistikmeldung generiert (und in die **biboAdmSyslogTable** eingeschrieben), welche detaillierte Informationen über die Verbindungen mit diesem WAN Partner enthält. (Einstellungen zum Speichern der Accounting Messages in eine Datei finden Sie in ***System*** ➜ ***External System Logging***.)

Back Route Verification Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion des **VPN Access** Gateways. Wenn Backroute Verification bei einem Interface aktiviert ist, werden über dieses eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über das gleiche Interface geroutet würden. Dadurch können Sie – auch ohne Filter – die Akzeptanz von Paketen mit gefälschten IP-Adressen verhindern.

Route Announce Diese Option ermöglicht die Einstellung, wann ggf. aktivierte Routing Protokolle (z.B. RIP) die für dieses Interface definierten IP Routen propagieren sollen.

Proxy Arp Mit Hilfe von ➤➤ **Proxy ARP** kann das Gateway ➤➤ **ARP**-Requests aus dem eigenen LAN stellvertretend für diesen spezifischen WAN Partner beantworten. Wenn ein Host im LAN eine Verbindung zu einem anderen Host im LAN oder zu einem WAN Partner aufbauen will, aber dessen Hardware-Adresse (MAC Adresse) nicht kennt, sendet er einen sogenannten ARP-Request als ➤➤ **Broadcast** ins Netz. Wenn auf dem Gateway Proxy ARP aktiviert ist und der gewünschte Ziel-Host z.B. über eine Host-Route 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.

Hinweis

Achten Sie darauf, dass beim definierten WAN Partner ebenfalls Proxy ARP aktiviert ist.

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

Feld	Wert
RIP Send	Ermöglicht Senden von RIP-Paketen über die Schnittstelle zum WAN Partner. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP Send und RIP Receive” auf Seite 53
RIP Receive	Ermöglicht Empfangen von RIP-Paketen über die Schnittstelle zum WAN Partner. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP Send und RIP Receive” auf Seite 53
IP Accounting	Ermöglicht Erzeugen von Accounting-Messages für z.B. ➤➤ **TCP-**, ➤➤ **UDP-** und ICMP-Sitzungen. Mögliche Werte: *on*, *off* (Defaultwert).
Back Route Verify	Aktiviert Backroute Verification für die Schnittstelle zum WAN Partner. Mögliche Werte: *on, off* (Defaultwert).
Route Announce	Mögliche Werte: ■ *up or dormant* (Defaultwert): Routen werden propagiert, wenn der Status des Interfaces *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.

Feld	Wert
Proxy Arp	Ermöglicht dem Gateway, ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen WAN Partner zu beantworten. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Proxy Arp” auf Seite 53
Van Jacobson Header Compression	Verringert die Größe der TCP/IP Pakete. Mögliche Werte: ■ *on*: VJHC aktiviert. ■ *off* (Defaultwert): VJHC deaktiviert.
Dynamic Name Server Negotiation	Definiert, ob das **VPN Access** Gateway IP-Adressen für ***Primary Domain Name Server, Secondary Domain Name Server, Primary WINS*** und ***Secondary WINS*** vom WAN Partner erhält oder diese zum WAN Partner schickt. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Dynamic Name Server Negotiation” auf Seite 54.

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

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

Wert	Bedeutung
none (Defaultwert)	Nicht aktiviert.
RIP V2 multicast	Nur für ***RIP Send*** Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9.
RIP V1 triggered	RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered ➤➤ **RIP**).

Wert	Bedeutung
RIP V2 triggered	RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. 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 (Defaultwert)	Deaktiviert Proxy ARP für diesen WAN Partner.
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.
yes (Defaultwert)	Die Bedeutung ist abhängig von der Einstellung in ***WAN PARTNER*** ➜ ***EDIT*** ➜ ***IP*** unter ***IP TRANSIT NETWORK***: ■ Wenn *dynamic client* ausgewählt wurde, sendet das **VPN Access** Gateway Name Server Adress-Anfragen zum WAN Partner. ■ Wenn *dynamic server* ausgewählt wurde, beantwortet das **VPN Access** Gateway Name Server Adress-Anfragen vom WAN Partner. ■ Wenn *yes* oder *no* ausgewählt wurde, antwortet das **VPN Access** Gateway, schickt aber keine Name Server Adress-Anfragen.
client (receive)	Das **VPN Access** Gateway sendet Name Server Adress-Anfragen zum WAN Partner.
server (send)	Das **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.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][ADD][BRIDGE]: Bridge Configuration (Filiale)            MyGateway


       Enable Bridging              no



            OK                                CANCEL
```

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**.

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, muss die Funktion im Feld ***BRIDGING*** für das jeweilige Ethernet-Interface des LAN aktiviert werden.

Um den spezifischen WAN Partner in das Bridging mit einzubeziehen, wird der Wert für ***ENABLE BRIDGING*** auf *yes* gestellt (Defaultwert ist *no*).

6 Untermenü Bridge

Index: WAN Partner

A

Advanced Settings 48
Authentication 11
Authentisierungsverhandlung 11

B

Back Route Verification 50
Back Route Verify 51
Bandwidth On Demand (=BOD) 22
Basic IP-Settings 37
Bridge 55
    Bridging-Modus 55

C

Callback 15, 17, 20
Calling Line Identification 7
Channel-Bundling 16, 18
Closed User Group 36
Compression 6, 7
CUG-Index 36

D

D-Channel Queue Length 26
Default Route 37, 40, 41
Delay after Connection Failure 16
Delay after Connection Failure (sec) 18
Destination IP-Address 43, 46
Destination Port 47, 48
Direction 34
Dynamic Name Server Negotiation 52, 54

E

Enable NAT 39, 41
Encapsulation 5, 6
Encryption 6
Encryption Key (RX) 27
Encryption Key (TX) 27
Encryption Key Negotiation 27
Erweitertes IP-Routing 44

Extended Interface Settings 22
Extended Routing 44

F

Flags 42

G

Gateway IP-Address 44
Gear Down Threshold 25
Gear Up Threshold 25
Geschlossene Benutzergruppe 36

I

Idle for Dynamic Short Hold (%) 17
IP 37
IP Accounting 50, 51
IP Transit Network 39
ISDN Ports to use 34

K

Keepalives 12

L

Layer 1 Protocol 16, 18, 21
Line Utilization Sample (sec) 25
Line Utilization Weighting 24
Link Qualitiy Monitoring 12
Local IP Address 39
Local PPP ID 11

M

Maximum Number of Dialup Channels 26
Metric 44, 46
Mode 24, 27, 46, 47
More Routing 42

N

Netmask 44, 46
Network 43, 44, 46
Number 33

P

Partner / Interface 46
Partner IP Address 39

Partner Name 5
Partner PPP ID 11
Partnername 3
PPP Password 11
Pro 42
Protocol 3, 47
Proxy Arp 50, 52, 53

R

Remote IP Address 40
Remote Netmask 40
Remote X.25 Address 19
RIP 49
RIP Receive 51, 52
RIP Send 51, 52
Route 37
Route Announce 50, 51
Route Type 43, 46
Routing-Einstellungen 37
Rufnummern des WAN Partners 33

S

Shorthold 15
Source Interface 47
Source IP-Address 47
Source Mask 47
Source Port 47, 48
Special Interface Types 19
State 3
Static Short Hold (sec) 17

T

TOS Mask 47
Total Number of Channels 19
Type of Service (TOS) 47

V

Van Jacobson Header Compression 52