

PPP

Copyright © 18. November 2004 Funkwerk Enterprise Communications GmbH
Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.0

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 Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

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 PPP	3
	Index: PPP	7



1 Menü PPP

im Folgenden werden die Felder des Menüs *PPP* beschrieben.

VPN Access 25 Setup Tool	Bintec Access Networks GmbH
[PPP]: PPP Profile Configuration	MyGateway
Authentication Protocol	CHAP + PAP + MS-CHAP
Radius Server Authentication	inband
PPP Link Quality Monitoring	no
PPPoE Ethernet Interface	disabled
SAVE	CANCEL

Das Menü enthält allgemeine ►► **PPP**-Einstellungen, die sich nicht nur auf einzelne WAN Partner beziehen, wie z. B. **AUTHENTICATION PROTOCOL**. Aufgrund dieser Einstellung führt das Gateway bei eingehenden Rufen eine Authentifizierungsverhandlung aus, wenn es die Calling Party Number nicht identifiziert (z. B. weil die Gegenstelle keine Calling Party Number signalisiert). Wenn die mit Hilfe des ausgeführten Authentisierungsprotokolls erhaltenen Daten (Passwort, Partner PPP ID) mit den Daten eines eingetragenen WAN Partners oder RADIUS Users übereinstimmen, akzeptiert das **VPN Access Gateway** den ankommenden Ruf.

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

Feld	Wert
Authenticaton Protocol	<p>Definiert die PPP-Authentisierungs-Protokolle, die das Gateway bei eingehenden Rufen ohne >> CLID anwenden darf.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>PAP</i>: nur PAP ■ <i>CHAP</i>: nur CHAP ■ <i>CHAP + PAP</i>: erst CHAP, dann PAP ■ <i>MS-CHAP</i>: nur MS-CHAP Version 1 ■ <i>CHAP + PAP + MS-CHAP</i> (Defaultwert): erst CHAP, bei Ablehnung anschließend das vom Anrufer gewollte Protokoll (MS-Chap Version 1 oder 2 möglich) ■ <i>MS-CHAP V2</i>: nur MS-CHAP Version 2 ■ <i>none</i>: keine PPP-Authentisierung.

Feld	Wert
Radius Server Authentication	<p>Einstellungen zur RADIUS Server Authentisierung. (RADIUS = Remote Authentication Dial In User Service).</p> <p>Folgende Reihenfolge wird bei der Authentisierung für eingehende Verbindungen unter Berücksichtigung von RADIUS angewendet: zunächst CLID, dann CLID mit RADIUS, danach PPP und daraufhin PPP mit RADIUS.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>inband</i> (Defaultwert): Nur Inband-RADIUS-Anfragen (PAP, CHAP, MS-CHAP V1 & V2) (d. h. PPP-Anfragen ohne Rufnummeridentifizierung) werden zum in IP → RADIUS SERVER definierten RADIUS Server geschickt. ■ <i>Calling Line Identification (CLID)</i>: Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummeridentifizierung) werden zum RADIUS Server geschickt. ■ <i>CLID + inband</i>: Beide RADIUS-Anfragenarten werden zum RADIUS Server geschickt (erst Outband-Anfragen, dann wenn nötig Inband-Anfragen). ■ <i>none</i>: Keine RADIUS-Anfragen werden versendet.

Feld	Wert
PPP Link Quality Monitoring	<p>Definiert, ob Link Quality Monitoring für PPP-Verbindungen durchgeführt wird (nur notwendig in Ausnahmefällen, z. B. mit Nokia Communicator).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ■ <i>no</i> (Defaultwert): Wird nicht durchgeführt. ■ <i>yes</i>: Die Verbindungsstatistiken werden in der ►► MIB-Tabelle pppLqmTable gespeichert.
PPPoE Ethernet Interface	<p>Definiert das Ethernet-Interface, das für PPPoE-Verbindungen vorgegeben wird. WAN-partnerspezifische Einstellungen haben Vorrang. Defaultwert ist <i>disabled</i>.</p>

Tabelle 1-1: Felder im Menü **PPP**



Index: PPP

A	Authenticaton Protocol	4
	Authentisierungsverhandlung	3
C	Calling Party Number	3
	CHAP	4
	CLID	3, 5
L	Link Quality Monitoring	6
M	MS-CHAP	4
P	PAP	4
	PPP Link Quality Monitoring	6
	PPPoE Ethernet Interface	6
R	RADIUS	5
	Radius Server Authentication	5

