

WAN PARTNER KONFIGURATION

Copyright © 24. Juni 2005 Funkwerk Enterprise Communications GmbH
Bintec Workshop
Version 0.9

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.funkwerk-ec.com.

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.funkwerk-ec.com

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.funkwerk-ec.com.

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	Einleitung	3
1.1	Szenario	3
1.2	Voraussetzungen	3
2	Konfiguration	5
2.1	Windows-Client Einwahl	5
2.1.1	Eigene Rufnummern	5
2.1.2	Benutzerkennung	6
2.1.3	Zeitanpassungen	7
2.1.4	IP-Adressen Vergabe	8
2.1.5	Proxy Arp und Pool ID	9
2.1.6	IP-Adressen Pool	11
2.2	Anbindung der Außenstelle	13
2.2.1	Eigene Rufnummern	13
2.2.2	Benutzerkennung	14
2.2.3	Zeitanpassungen	15
2.2.4	Ausgehende Rufnummer	16
2.2.5	IP-Adressen Konfiguration	17
3	Ergebnis	19
3.1	Test	19
3.2	Konfigurationsschritte im Überblick	20



1 Einleitung

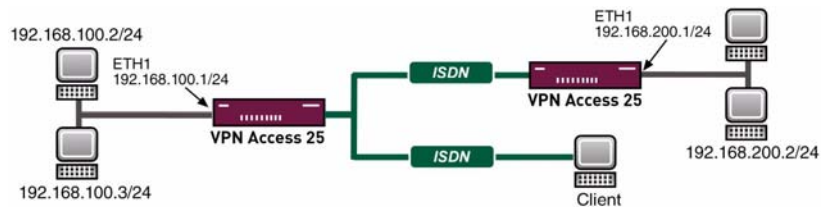
Im Folgenden wird die Konfiguration von WAN Partnern beschrieben.

Sie wählen sich über ISDN von einem Windows Rechner aus in das Firmennetzwerk ein und erhalten eine IP-Adresse aus dem IP-Subnetz.

Zudem konfigurieren Sie eine LAN Kopplung über ISDN zu einer Außenstelle, um auf das Remotenetz zugreifen zu können.

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.1 Szenario



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Eine IP-Adresse auf Ihrem LAN-Interface.
- Ein Bootimage ab Version 7.1.1.
- Der Bintec Router muss an einem ISDN Anschluss angeschlossen sein.
- Sie benötigen mindestens ein MSN.

2 Konfiguration

Um WAN Partner zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen: **WAN PARTNER → ADD**.

2.1 Windows-Client Einwahl

2.1.1 Eigene Rufnummern

Wenn Sie Ihren Router am ISDN Angeschlossen haben, konfigurieren Sie Ihre eigenen Rufnummern (MSN) im WAN Interface. Dazu gehen Sie in folgendes Menü: **ISDN S0 → INCOMING CALL ANSWERING → ADD**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[SLOT 0 UNIT 4 ISDN BRI] [INCOMING] [EDIT]	Zentrale
Item	PPP (routing)
Number	100100
Mode	right to left
Bearer	any
SAVE	CANCEL
Enter string, max length = 42 chars	

Folgende Felder sind relevant:

Feld	Bedeutung
Item	Hier können Sie den Dienst auswählen, der auf Ihre eigene Rufnummer reagiert.
Number	Tragen Sie in dieses Feld Ihre eigene Rufnummer (MSN) ein.

Tabelle 2-1: Relevante Felder in **ISDN S0 → INCOMING CALL ANSWERING → ADD**

Gehen Sie folgendermaßen vor, um einen Eintrag zu konfigurieren:

- **ITEM** stellen Sie für Datenverbindungen auf *PPP (routing)*.
- Unter **NUMBER** tragen Sie Ihre Rufnummer ein z.B. *100100*.



Hinweis

Sollten Sie nur eine Rufnummer an dem Anschluss zur Verfügung haben, die Sie allerdings auch zum telefonieren brauchen, können Sie den Bearer auf data stellen.

Um einen WAN Partner hinzuzufügen, gehen Sie in folgendes Menü: **WAN PARTNER → ADD**.

Tragen Sie unter **PARTNER NAME** einen Namen ein für die Verbindung z.B. *Client Einwahl*.

2.1.2 Benutzererkennung

Konfigurieren Sie jetzt die Authentifizierung, indem Sie in folgendes Menü gehen: **WAN PARTNER → ADD → PPP**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [PPP]: PPP Settings (Client Einwahl)	Zentrale
Authentication	CHAP + PAP
Partner PPP ID	Einwahl
Local PPP ID	
PPP Password	geheim
Keepalives	off
Link Quality Monitoring	off
OK	CANCEL

Folgende Felder sind relevant:

Feld	Bedeutung
Authentication	Wählen Sie das Protokoll aus, das Benutzernamen und Kennwort überprüft.
Partner PPP ID	Geben Sie hier für die Einwahl den Benutzernamen an.
PPP Password	Tragen Sie hier Ihr gemeinsames Passwort ein.

Tabelle 2-2: Relevante Felder in **WAN PARTNER → ADD → PPP**

Gehen Sie folgendermaßen vor, um einen Eintrag zu konfigurieren:

- Das Feld **AUTHENTICATION** stellen Sie auf **CHAP + PAP**.
- Unter **PARTNER PPP ID** tragen Sie den Benutzernamen ein z.B. *Einwahl*.
- Bei **PPP PASSWORD** wird z.B. *geheim* eingetragen.



Hinweis

Der Benutzername den Sie hier angeben ist kein Anmeldekonto von Windows, sondern lediglich für die Verbindung zum Router gedacht.

2.1.3 Zeitanpassungen

Korrigieren Sie die Zeit, wie lange die Verbindung aufrecht erhalten bleibt, obwohl keine Daten mehr transportiert werden.

- Gehen Sie zu **WAN PARTNER → ADD → ADVANCED SETTINGS**.

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[WAN] [ADD] [ADVANCED]: Advanced Settings (Client Einwahl)   Zentrale

  Callback                                           no
  Static Short Hold (sec)                            120
  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

Use <Space> to select

```

Folgendes Feld ist relevant:

Feld	Bedeutung
Static Short Hold (sec)	Wenn keine Daten übertragen werden, bleibt die Verbindung solange bestehen, wie Sie hier konfiguriert haben.

Tabelle 2-3: Relevantes Feld in **WAN PARTNER → ADD → ADVANCED SETTINGS**

Gehen Sie folgendermaßen vor:

- Tragen Sie in das Feld **STATIC SHORT HOLD (SEC)** z.B. den Wert **120** ein.

2.1.4 IP-Adressen Vergabe

Damit der Windows-Client eine IP-Adresse bei der Einwahl erhält, müssen Sie in folgendes Menü gehen: **WAN PARTNER → ADD → IP → BASIC IP-SETTINGS**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [IP] [BASIC]: IP-Settings (Client Einwahl)	Zentrale
IP Transit Network	dynamic server
SAVE	CANCEL

Folgendes Feld ist relevant:

Feld	Bedeutung
IP Transit Network	Hier konfigurieren Sie den IP-Adressen Bereich der Verbindung.

Tabelle 2-4: Relevantes Feld in **WAN PARTNER → ADD → IP → BASIC IP-SETTINGS**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Stellen Sie den Punkt **IP TRANSIT NETWORK** auf *dynamic server*.

2.1.5 Proxy Arp und Pool ID

Da Sie eine IP-Adresse aus dem selben Subnetz erhalten wo Sie drauf zugreifen, müssen Sie Proxy Arp einschalten.

Gehen Sie dazu in folgendes Menü: **WAN PARTNER → ADD → ADVANCED SETTINGS**.

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[WAN] [ADD] [IP] [ADVANCED]: Advanced Settings (Client Einwahl)  Zentrale

RIP Send                                               none
RIP Receive                                            none

IP Accounting                                          off
Back Route Verify                                     off
Route Announce                                        up or dormant
Proxy Arp                                             on (up only)

Van Jacobson Header Compression                       off
Dynamic Name Server Negotiation                      yes
IP Address Pool                                       0

OK                                                    CANCEL

Use <Space> to select

```

Folgende Felder sind relevant:

Feld	Bedeutung
Proxy Arp	Der Router antwortet stellvertretend für den eingewählten Client auf ARP Requests.
IP Address Pool	Dies ist die Pool ID, wo der IP-Address Pool hinterlegt wird.

Tabelle 2-5: Relevante Felder in **WAN PARTNER → ADD → ADVANCED SETTINGS**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Bei **IP ADDRESS POOL** tragen Sie eine freie Pool ID ein z.B. 0.
- Den Punkt **PROXY ARP** stellen Sie auf *on (up only)*.

Wenn Sie **PROXY ARP** nutzen, müssen Sie diese Funktion in allen beteiligten Interfaces einschalten. In diesem Beispiel im WAN Partner und im LAN Interface.

Gehen Sie in Ihr LAN Interface, um Proxy Arp einzuschalten: **ETHERNET UNIT 1 → ADVANCED SETTINGS**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[SLOT 0 UNIT 1 ETH] [ADVANCED]: Advanced Settings	Zentrale
RIP Send	none
RIP Receive	none
IP Accounting	off
Proxy Arp	on
Back Route Verify	off
SAVE	CANCEL
Use <Space> to select	

Folgendes Feld ist relevant:

Feld	Bedeutung
Proxy Arp	Der Router antwortet stellvertretend für den eingewählten Client auf Arp Requests.

Tabelle 2-6: Relevantes Feld in **ETHERNET UNIT 1 → ADVANCED SETTINGS**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Den Punkt **PROXY ARP** stellen Sie auf *on*.

2.1.6 IP-Adressen Pool

Jetzt müssen Sie noch den Pool mit der IP-Adresse anlegen, die der Client bei der Einwahl erhält. Gehen Sie dazu in folgendes Menü: **IP → IP ADDRESS POOL WAN (PPP) → ADD**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[SLOT 0 UNIT 1 ETH] [ADVANCED]: Advanced Settings	Zentrale
Pool ID	0
IP Address	192.168.100.10
Number of consecutive addresses	1
SAVE	CANCEL
Enter integer value	

Folgende Felder sind relevant:

Feld	Bedeutung
Pool ID	Dies ist die Pool ID, die Sie im WAN PARTNER → IP → ADVANCED SETTINGS angegeben haben.
IP Address	Hier tragen Sie die IP-Adresse ein, die der Client bei der Einwahl erhält.
Number of consecutive address	Bestimmen Sie hier die Größe des IP-Adressen Pools.

Tabelle 2-7: Relevante Felder in **IP → IP ADDRESS POOL WAN (PPP) → ADD**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Unter **POOL ID** tragen Sie z.B. 0 ein.
- Bei **IP ADDRESS** geben Sie z.B. 192.168.100.10 an.
- **NUMBER OF CONSECUTIVE ADDRESSES** steht auf 1.

2.2 Anbindung der Außenstelle

2.2.1 Eigene Rufnummern

Wenn Sie Ihren Router am ISDN Angeschlossen haben, konfigurieren Sie Ihre eigenen Rufnummern (MSN) im WAN Interface. Dazu gehen Sie in folgendes Menü: **ISDN S0 → INCOMING CALL ANSWERING → ADD**.

VPN Access 25 Setup Tool		BinTec Access Networks GmbH	
[SLOT 0 UNIT 4 ISDN BRI] [INCOMING] [EDIT]		Zentrale	
Item	Number	Mode	Bearer
	100100	right to left	any
SAVE			CANCEL
Enter string, max length = 42 chars			

Folgende Felder sind relevant:

Feld	Bedeutung
Item	Hier können Sie den Dienst auswählen, der auf Ihre eigene Rufnummer reagiert.
Number	Tragen Sie in dieses Feld Ihre eigene Rufnummer (MSN) ein.

Tabelle 2-8: Relevante Felder in **ISDN S0 → INCOMING CALL ANSWERING → ADD**

Gehen Sie folgendermaßen vor, um einen Eintrag zu konfigurieren:

- **ITEM** stellen Sie für Datenverbindungen auf *PPP (routing)*.
- Unter **NUMBER** tragen Sie Ihre Rufnummer ein z.B. *100100*.

Um einen WAN Partner hinzuzufügen, gehen Sie in folgendes Menü: **WAN PARTNER → ADD**.

Tragen Sie unter Partner Name einen Namen ein für die Verbindung z.B. Aussenstelle.

2.2.2 Benutzererkennung

Konfigurieren Sie jetzt die Authentifizierung, indem Sie in folgendes Menü gehen: **WAN PARTNER → ADD → PPP**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [PPP]: PPP Settings (Aussenstelle)	Zentrale
Authentication	CHAP + PAP
Partner PPP ID	Aussenstelle
Local PPP ID	Zentrale
PPP Password	Secret
Keepalives	off
Link Quality Monitoring	off
OK	CANCEL

Folgende Felder sind relevant:

Feld	Bedeutung
Authentication	Wählen Sie das Protokoll aus, das Benutzername und Kennwort überprüft.
Partner PPP ID	Tragen Sie hier einen Benutzernamen ein, falls sich die Gegenstelle bei Ihnen einwählt.
Local PPP ID	Tragen Sie hier einen Benutzernamen ein, falls Sie sich bei der Gegenstelle einwählen.
PPP Password	Hier wird Ihr gemeinsames Passwort eingetragen.

Tabelle 2-9: Relevante Felder in **WAN PARTNER → ADD → PPP**

Gehen Sie folgendermaßen vor, um einen Eintrag zu konfigurieren:

- Das Feld **AUTHENTICATION** stellen Sie auf **CHAP + PAP**.
- Unter **PARTNER PPP ID** tragen Sie z.B. *Aussenstelle* ein.
- Unter **LOCAL PPP ID** tragen Sie z.B. *Zentrale* ein.
- Bei **PPP PASSWORD** wird z.B. *Secret* eingetragen.

2.2.3 Zeitanpassungen

Korrigieren Sie die Zeit, wie lange die Verbindung aufrechterhalten bleibt, obwohl keine Daten mehr transportiert werden.

- Gehen Sie zu **WAN PARTNER → ADD → ADVANCED SETTINGS**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [ADVANCED]: Advanced Settings (Aussenstelle)	Zentrale
Callback	no
Static Short Hold (sec)	120
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
Use <Space> to select	

Folgendes Feld ist relevant:

Feld	Bedeutung
Static Short Hold (sec)	Wenn keine Daten übertragen werden, bleibt die Verbindung solange bestehen, wie Sie hier konfiguriert haben.

Tabelle 2-10: Relevantes Feld in **WAN PARTNER → ADD → ADVANCED SETTINGS**

Gehen Sie folgendermaßen vor:

- Tragen Sie in das Feld **STATIC SHORT HOLD (SEC)** z.B. den Wert **120** ein.

2.2.4 Ausgehende Rufnummer

Damit die Zentrale die Aussenstelle über ISDN erreicht, müssen Sie in folgendem Menü eine Rufnummer hinzufügen: **WAN PARTNER → ADD → WAN NUMBERS → ADD**.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [WAN NUMBERS] [ADD]: Add or Change	Zentrale
WAN Numbers (Aussenstelle)	
Number	200200
Direction	outgoing
Advanced Settings >	
ISDN Ports to use	<X> Slot 0 Auxiliary <X> Slot 0 ISDN S0
SAVE	CANCEL
Enter string, max length = 40 chars	

Folgendes Feld ist relevant:

Feld	Bedeutung
Number	Hier tragen Sie die Rufnummer der Gegenseite ein.

Tabelle 2-11: Relevantes Feld in **WAN PARTNER → ADD → WAN NUMBERS → ADD**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Tragen Sie in das Feld **NUMBER** z.B. **200200** ein.

2.2.5 IP-Adressen Konfiguration

Gehen Sie in folgendes Menü, um das IP-Netz der Gegenstelle anzugeben:

WAN PARTNER → ADD → IP → BASIC IP-SETTINGS.

VPN Access 25 Setup Tool	BinTec Access Networks GmbH
[WAN] [ADD] [IP] [BASIC]: IP-Settings (Aussenstelle)	Zentrale
IP Transit Network	no
Local IP Address	192.168.100.1
Default Route	no
Remote IP Address	192.168.200.0
Remote Netmask	255.255.255.0
SAVE	CANCEL

Folgende Felder sind relevant:

Feld	Bedeutung
IP Transit Network	Bestimmen Sie hier ob Sie ein Transitnetz nutzen.
Local IP Address	Geben Sie Ihre IP-Adresse vom LAN-Interface an.
Remote IP Address	Hier tragen Sie das IP-Netz der Gegenstellen ein.
Remote Netmask	Dies ist die Subnetzmaske, die zur Remote IP Address gehört.

Tabelle 2-12: Relevante Felder in **WAN PARTNER → ADD → IP → BASIC IP-SETTINGS**

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Das **IP TRANSIT NETWORK** stellen Sie auf *no*.
- Unter **LOCAL IP ADDRESS** tragen Sie z.B. *192.168.100.1* ein.

- Bei **REMOTE IP ADDRESS** geben Sie z.B. *192.168.200.0* an.
- In das Feld **REMOTE NETMASK** tragen Sie z.B. *255.255.255.0* ein.



Bedenken Sie, dass dies eine Beispielkonfiguration auf Seiten der Zentrale ist. Konfigurieren Sie die gleichen Schritte in der Außenstelle mit den dort verwendeten Werten.

3 Ergebnis

Sie haben eine Remoteeinwahl von einem Windows Client auf den Bintec Router konfiguriert und erhalten bei der Einwahl eine IP-Adresse aus demselben Subnetz. Zudem haben Sie Ihre Außenstelle über ISDN an die Zentrale angebunden.

3.1 Test

Um die Verbindungen zu überprüfen, rufen Sie die Eingabeaufforderung auf einem Rechner in der Außenstelle oder auf dem Einwahlrechner auf und geben einen Ping auf das zentrale Netz ab: z.B. `ping 192.168.100.2`.

Sie müssten dann folgende Meldungen erhalten:

```
Ping wird ausgeführt für 192.168.100.1 mit 32 Bytes Daten:
Antwort von 192.168.100.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.100.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.100.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.100.1: Bytes=32 Zeit<1ms TTL=63

Ping-Statistik für 192.168.100.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca.
    Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

3.2 Konfigurationsschritte im Überblick

Remoteeinwahl

FELD	MENÜ	WERT
Item	ISDN S0 → INCOMING CALL ANSWERING → ADD	PPP (routing)
Number	ISDN S0 → INCOMING CALL ANSWERING → ADD	z.B. 100100
Partner Name	WAN PARTNER → ADD	z.B. Client Einwahl
Authentication	WAN PARTNER → ADD → PPP	z.B. CHAP + PAP
Partner PPP ID	WAN PARTNER → ADD → PPP	z.B. Einwahl
PPP Password	WAN PARTNER → ADD → PPP	z.B. geheim
Static Short Hold (sec)	WAN PARTNER → ADD → ADVANCED SETTINGS	z.B. 120
IP Transit Network	WAN PARTNER → ADD → IP → BASIC IP-SETTINGS	dynamic server
Proxy Arp	WAN PARTNER → ADD → ADVANCED SETTINGS	z.B. 0
IP Address Pool	WAN PARTNER → ADD → ADVANCED SETTINGS	on (up only)
Proxy Arp	ETHERNET UNIT 1 → ADVANCED SETTINGS	on
Pool ID	IP → IP ADDRESS POOL WAN (PPP) → ADD	z.B. 0
IP Address	IP → IP ADDRESS POOL WAN (PPP) → ADD	z.B. 192.168.100.10
Number of consecutive addresses	IP → IP ADDRESS POOL WAN (PPP) → ADD	1

LAN Kopplung

FELD	MENÜ	WERT
Item	ISDN S0 → INCOMING CALL ANSWERING → ADD	PPP (routing)
Number	ISDN S0 → INCOMING CALL ANSWERING → ADD	z.B. 100100
Partner Name	WAN PARTNER → ADD	z.B. Aussenstelle
Authentication	WAN PARTNER → ADD → PPP	z.B. CHAP + PAP

FELD	MENÜ	WERT
Partner PPP ID	WAN PARTNER → ADD → PPP	z.B. Aussenstelle
Local PPP ID	WAN PARTNER → ADD → PPP	z.B. Zentrale
PPP Password	WAN PARTNER → ADD → PPP	z.B. Secret
Static Short Hold (sec)	WAN PARTNER → ADD → ADVANCED SETTINGS	z.B. 120
Number	WAN PARTNER → ADD → WAN NUMBERS → ADD	z.B. 200200
IP Transit Network	WAN PARTNER → ADD → IP → BASIC IP-SETTINGS	no
Local IP Address	WAN PARTNER → ADD → IP → BASIC IP-SETTINGS	z.B. 192.168.100.1
Remote IP Address	WAN PARTNER → ADD → IP → BASIC IP-SETTINGS	z.B. 192.168.200.0
Remote Netmask	WAN PARTNER → ADD → IP → BASIC IP-SETTINGS	z.B. 255.255.255.0

